M. Postnikov

Lectures in Geometry

SEMESTER V

Lie Groups and Lie Algebras

$$\begin{tikzcd}
\widetilde{G} \arrow[r, "\omega"] \arrow[d, "\pi"] & \widetilde{G/H} \arrow[d, "\rho"] \\
G \arrow[r] & G/H
\end{tikzcd}$$

Mir Publishers Moscow

This textbook like the rest of the series is compiled from lectures delivered by the author to students at Moscow State University.
The audience was made up of final year students and postgraduates, and as a consequence, a certain level of knowledge (for example, the properties of manifolds) is assumed.
The lectures fall into five parts. The first covers the basic concepts of Lie groups, Lie algebras, and the Lie algebra of a given Lie group. The second part deals with "locality theory", the third generalizes these ideas.
The first three sections could be used as a foundation course in Lie algebras for beginners.
The fourth part considers Lie subgroups and Lie factor groups.
The final part has a purely algebraic character, and is practically independent of the preceding four parts; it considers a proof of Ado's theorem, which is interesting in itself.
This book will be useful for mathematics students taking courses in Lie algebras, because it contains all the major results and proofs in compact and accessible form.

ИЗДАТЕЛЬСТВО · МИР ·

М. М. ПОСТНИКОВ

ЛЕКЦИИ ПО ГЕОМЕТРИИ

СЕМЕСТР 5

ГРУППЫ И АЛГЕБРЫ ЛИ

МОСКВА «НАУКА»

Главная редакция физико-математической
литературы

M. POSTNIKOV

LECTURES IN GEOMETRY

SEMESTER V

LIE GROUPS AND LIE ALGEBRAS

Translated from the Russian by Vladimir Shokurov

MIR PUBLISHERS
MOSCOW

First published 1986
Revised from the 1982 Russian edition

На английском языке

CONTENTS

Preface 10

Lecture 1 15

Smooth and topological groups. Relaxing the conditions defining Lie groups. Examples of Lie groups. Cayley transformation. Further examples of Lie groups. Connected and arcwise connected spaces and groups. Reduction of any smooth groups to connected groups. Examples of connected Lie groups

Lecture 2 33

Left-invariant vector fields. Parallelizability of Lie groups. Integral curves of left-invariant vector fields and one-parameter subgroups. Lie functor. An example: a group of invertible elements of an associative algebra. Functions with values in an associative algebra. One-parameter subgroups of the group $G(\mathcal{A})$

Lecture 3 51

Matrix Lie groups admitting the Cayley construction. A generalization of the Cayley construction. Groups possessing ln-images. Lie algebras. Examples of Lie algebras. Lie algebras of vector fields. The Lie algebra of a Lie group. An example: the Lie algebra of a group of invertible elements of an associative algebra. Locally isomorphic Lie groups. Local Lie groups. Lie functor on the category of local Lie groups

Lecture 4 71

The exponent of a linear differential operator. A formula for the values of smooth functions in the normal neighbourhood of the identity of a Lie group. A formula for the values of smooth functions on the product of two elements. The Campbell-Hausdorff series and Dynkin polynomials. The convergence of a Campbell-Hausdorff series. The reconstruction of a local Lie group from its Lie algebra. Operations in the Lie algebra of a Lie group and one-parameter subgroups. Differentials of internal automorphisms. The differential of an exponential mapping. Canonical coordinates. The uniqueness of the structure of a Lie group. Groups without small subgroups and Hilbert's fifth problem

Lecture 5 98

Free associative algebras. Free Lie algebras. The basic lemma. The universal enveloping algebra. The embedding of a Lie algebra into its universal enveloping algebra. Proof of the fact that the algebra I $\langle X \rangle$ is free. The Poincaré-Birkhoff-Witt theorem. Tensor products of vector spaces and of algebras. Hopf algebras

Lecture 6 116

The Friedrichs theorem. The proof of Statement **B** of Lecture 4. The Dynkin theorem. The linear part of a Campbell-Hausdorff series. The convergence of a Campbell-Hausdorff series. Lie group algebras. The equivalence of the categories of local Lie groups and of Lie group algebras. Isomorphism of the categories of Lie group algebras and of Lie algebras. Lie's third theorem

Lecture 7 134

Local subgroups and subalgebras. Invariant local subgroups and ideals. Local factor groups and quotient algebras. Reducing smooth local groups to analytic ones. Pfaffian systems. Subfiberings of tangent bundles. Integrable subfiberings. Graphs of a Pfaffian system. Involutory subfiberings. The complete univalence of a Lie functor. The involutedness of integrable subfiberings. Completely integrable subfiberings

Lecture 8 159

Coverings. Sections of coverings. Pointed coverings. Coamalgams. Simply connected spaces. Morphisms of coverings. The relation of quasi-order in the category of pointed coverings. The existence of simply connected coverings. Questions of substantiation. The functorial property of a universal covering

Lecture 9 183

Smooth coverings. Isomorphism of the categories of smooth and topological coverings. The existence of universal smooth coverings. The coverings of smooth and topological groups. Universal coverings of Lie groups. Lemmas on topological groups. Local isomorphisms and coverings. The description of locally isomorphic Lie groups

Lecture 10 197

Local isomorphisms and isomorphisms of localizations. The Cartan theorem. A final diagram of categories and functors. Reduction of the Cartan theorem. The globalizability of embeddable local groups. Reducing the Cartan theorem to the Ado theorem

Lecture 11 208

Submanifolds of smooth manifolds. Subgroups of Lie groups. Integral manifolds of integrable subfiberings. Maximal integral manifolds. The idea of the proof of Theorem 1. The local structure of submanifolds. The uniqueness of the structure of a locally rectifiable submanifold with a countable base. Submanifolds of manifolds with a countable base. Connected Lie groups have a countable base. The local rectifiability of maximal integral manifolds. The proof of Theorem 1

Lecture 12 228

Alternative definitions of a subgroup of a Lie group. Topological subgroups of Lie groups. Closed subgroups of Lie

groups. Algebraic groups. Groups of automorphisms of algebras. Groups of automorphisms of Lie groups. Ideals and invariant subgroups. Quotient manifolds of Lie groups. Quotient groups of Lie groups. The calculation of fundamental groups. The simple-connectedness of groups SU (n) and Sp (n). The fundamental group of a group $\mathrm{U}(n)$

Lecture 13 247

The Clifford algebra of a quadratic functional. $\mathbb{Z}_2$-graduation of a Clifford algebra. More about tensor multiplication of vector spaces and algebras. Decomposition of Clifford algebras into a skew tensor product. The basis of a Clifford algebra. Conjugation in a Clifford algebra. The centre of a Clifford algebra. A Lie group Spin(n). The fundamental group of a group SO(n). Groups Spin(n) with $n \leqslant 4$. Homomorphism χ. The group Spin(6). The group Spin(5). Matrix representations of Clifford algebras. Matrix representations of groups Spin(n). Matrix groups in which groups Spin(n) are represented. Reduced representations of groups Spin(n). Additional facts from linear algebra

Lecture 14 286

Doubling of algebras. Metric algebras. Normed algebras. Automorphisms and differentiations of metric algebras. Differentiations of a doubled algebra. Differentiations and automorphisms of the algebra $\mathbb{H}$. The algebra of octaves. The Lie algebra $\mathfrak{g}_2^{\mathbb{C}}$. Structural constants of the Lie algebra $\mathfrak{g}_2^{\mathbb{C}}$. Representation of the Lie algebra $\mathfrak{g}_2^{\mathbb{C}}$ by generators and relations

Lecture 15 306

Identities in the octave algebra $\mathbb{C}$a. Subalgebras of the octave algebra $\mathbb{C}$a. The Lie group G_2. The triplicity principle for the group Spin(8). The analogue of the triplicity principle for the group Spin(9). The Albert algebra Al. The octave projection plane

Lecture 16 327

Scalar products in the algebra Al. Automorphisms and differentiations of the algebra Al. Adjoint differentiations of the algebra Al. The Freudenthal theorem. Consequences of the Freudenthal theorem. The Lie group F_4. The Lie algebra $\mathfrak{f}_4$. The structure of the Lie algebra $\mathfrak{f}_4^{\mathbb{C}}$

Lecture 17 346

Solvable Lie algebras. The radical of a Lie algebra. Abelian Lie algebras. The centre of a Lie algebra. Nilpotent Lie algebras. The nilradical of a Lie algebra. Linear Lie nilalgebras. The Engel theorem. Criteria of nilpotency. Linear irreducible Lie algebras. Reductive Lie algebras. Linear solvable Lie algebras. The nilpotent radical of a Lie algebra

Lecture 18 360

Trace functional. Killing's functional. The trace functional of a representation. The Jordan decomposition of a linear operator. The Jordan decomposition of the adjoint operator. The Cartan theorem on linear Lie algebras. Proving Cartan's criterion for the solvability of a Lie algebra. Linear Lie algebras with a nonsingular trace functional. Semisimple Lie algebras. Cartan's criterion for semisimplicity. Casimir operators

Lecture 19 377

Cohomologies of Lie algebras. The Whitehead theorem. The Fitting decomposition. The generalized Whitehead theorem. The Whitehead lemmas. The Weyl complete reducibility theorem. Extensions of Abelian Lie algebras

Lecture 20 391

The Levi theorem. Simple Lie algebras and simple Lie groups. Cain and unimodular groups. Schur's lemma. The centre of a simple matrix Lie group. An example of a nonmatrix Lie group. De Rham cohomologies. Cohomologies of the Lie algebras of vector fields. Comparison between the cohomologies of a Lie group and its Lie algebra

Lecture 21 404

Killing's functional of an ideal. Some properties of differentiations. The radical and nilradical of an ideal. Extension of differentiations to a universal enveloping algebra. Ideals of finite codimension of an enveloping algebra. The radical of an associative algebra. Justification of the inductive step of the construction. The proof of the Ado theorem. Conclusion

Supplement to the English Translation. *Proof of the Cartan theorem by V. V. Gorbatsevich*) 418

Bibliography 431

Subject Index 433

PREFACE

The theory of Lie groups relies on Cartan's theorem on the equivalence of the category of simply connected Lie groups to that of Lie algebras. This book presents the proof of the Cartan theorem and the main results. The branches of the theory of Lie groups which rest on the Cartan theorem remain outside the limits of our exposition. The theory of Lie algebras has been developed to an extent necessary for the Cartan theorem to be proved.

This book like the previous ones of this series* is a nearly faithful record of the lectures delivered by the author at Moscow University to students (and postgraduates) of the Faculty of Mathematical Mechanics. However, while books I and II were based on lectures of a compulsory course, this book is a record of an elective course, which makes it essentially different in a number of respects.

Designed for senior and postgraduate students (these lectures conditionally belong to the fifth semester since students who attended the lectures were uniformly distributed over all senior courses) the lectures allowed the

---

* M. M. Postnikov. *Lectures in Geometry*: *Semester* 1. *Analytic Geometry*, Mir Publishers, Moscow, 1981), *Semester* 2. *Linear Algebra and Differential Geometry*. Mir Publishers, Moscow, 1982). (Referred to as I and II respectively in what follows.)

presentation during teaching period of 90 minutes of much more material than had been possible in books I and II intended for first-year students. The volume of the lectures was increased due to the fact that they became two hours long (120 minutes) while the breaks became shorter and the lectures continued after the bell had rung. All this almost doubled the actual volume of each lecture. Of course, with a less intense pace of teaching, under the conditions of, say, a one-year and not a one-semester course, each lecture virtually extends into a lecture and a half or even two lectures. This book, therefore may be better regarded as a record of a one-year elective course (but I managed sometimes—under particularly favourable circumstances—even in one semester), especially since for various reasons it is usually possible to give not more than twelve or thirteen lectures during a semester, although the curriculum requires eighteen lectures.

Because of the acute shortage of time, in teaching an elective course, one has more often than in a compulsory course to confine oneself to the mere idea of a proof, leaving the details for the students to prove. It suffices to formulate, with references to the literature, the auxiliary statements from other branches of mathematics and merely to describe the examples illustrating the general theory, leaving their detailed analysis to the students. When, however, a lecture is committed to paper, it is not necessary to meet these demands, and what is more, all the proofs should be carried out in detail, the examples completely analysed and constructing the "outside" lemmas proved. This sometimes leads to a two or three-fold increase in the volume of a recorded lecture.

Every lecturer, presupposing a certain stock of knowledge in his students, is nevertheless compelled to recall at least in short particularly important facts. In written form one has

to expand them into a systematic, sometimes rather large, section for the reader's convenience.

This accounts for the surprisingly large volume of some of the lectures in the book. Yet, with account of the foregoing, each lecture here is in fact a record of a real lecture (within which occur self-understood shifts of the initial and terminal pieces of neighbouring lectures).

All the lectures virtually break down into five series. The first series (Lectures 1, 2 and 3) introduces, and explains by way of examples, the basic notions: Lie groups, Lie algebras and the Lie algebras of a given Lie group.

The next series (Lectures 4 to 7) is devoted to the "local theory" of Lie groups, Lectures 4 and 6 establish the equivalence of the category of Lie algebras to that of analytic local Lie groups. The necessary algebraic tools are developed in Lecture 5. In Lecture 7, it is proved that analyticity may in fact be assumed without loss of generality. Local subgroups and local factor groups are also considered here.

Extension from the local to the global theory is carried out in Lectures 8, 9 and 10. Lecture 8 presents the theory of coverings (in the sense of Chevalley, i.e. "without paths"). In Lecture 9 a universal covering group is constructed. In Lecture 10 the Cartan theorem is formulated and discussed. No proof of the theorem is constructed, it is only reduced to the Ado theorem on the existence of an exact linear representation for any Lie algebra.

These three series may serve as a miniature course in the theory of Lie groups for beginners.

Lectures 11 and 12 expound subgroups and quotient groups of Lie groups. Lecture 13 is devoted to Clifford algebras and spinor groups. For the first time in educational literature, particular Lie groups G_2 and F_4 together with the necessary algebraic tools are considered in detail in Lectures 14 to 16.

The last lectures, 17 to 21, are of a purely algebraic character and are practically independent of all the foregoing material (except for Lecture 20 which stands somewhat by itself). Formally they are devoted to the proof of the Ado theorem, but in fact they comprise a very large fragment of the theory of Lie algebras (Cartan's criteria for solvability and semisimplicity, the Whitehead lemmas, the Weyl and Levi theorems) which is of independent interest as well.

In conclusion I wish to express my gratitude to V.L. Popov whose contribution to the improvement of the original manuscript of the book has greatly surpassed the usual duties of an editor.

M.M. Postnikov

Lecture I

Smooth and topological groups • Relaxing the conditions defining Lie groups • Examples of Lie Groups • Cayley transformation • Further examples of Lie groups. Connected and arcwise connected spaces and groups • Reduction of any smooth groups to connected groups • Examples of connected Lie groups

Let G be at the same time a group and a smooth manifold*.

Definition 1. The group G is said to be a *Lie group* (or a *smooth group*) if the mappings

$$G \times G \to G, \quad (a, b) \mapsto ab, \tag{1}$$

and

$$G \to G, \quad a \mapsto a^{-1}, \tag{2}$$

are smooth mappings.

Let G and H be Lie groups. The mapping $G \to H$ is said to be a *morphism* of Lie groups (or their *smooth homomorphism*) if it is their homomorphism as abstract groups and their smooth mapping as manifolds.

All Lie groups and all their homomorphisms form a category. We shall denote this category as GR-DIFF.

---

* We assume known the preliminaries of smooth manifold theory envisaged by the syllabus of the compulsory course of geometry for the third semester of the Faculty of Mathematical Mechanics of Moscow State University. To familiarize oneself with them before Semester 3 of these "lectures" appears in print the reader may use any of the numerous available expositions.

For the necessary information on group theory see, for example, A.I. Kostrikin, *Introduction to Algebra*, Moscow, Nauka Publishers, 1978.

Remark 1. There is a countable family of categories GR-DIFF depending on C^r-smoothness (where either $2 \leqslant r \leqslant \infty$ or $r = \omega$) we require of the manifolds under consideration. In fact, however, practically nothing depends on r, since, as is shown in Lecture 7, any C^r-smooth group is C^r-isomorphic to the analytic (class C^ω) group.

Remark 2. Some authors find slight differences between Lie groups and smooth (in particular analytic) groups. We shall consider both terms to be synonymous, preferring the former as more common and traditional.

Similarly the group G which is at the same time a topological space is said to be a *topological group* if mappings (1) and (2) are continuous for it. The homomorphism $G \to H$ of topological groups is said to be *continuous* if it is a continuous mapping. Topological groups and their continuous homomorphisms constitute the category GR-TOP.

Recall that the topological space M is said to be *Hausdorff* (or *separable*) if any two of its distinct points have disjoint neighbourhoods, i.e. if, in other words, the *diagonal* Δ (the subset of the product $M \times M$ which consists of points of the form (x, x), $x \in M$) is closed in M. A topological group (as well as a smooth manifold) should not necessarily be Hausdorff.

Lemma 1. *A topological group G is Hausdorff if and only if its identity is closed.*

Proof. In a Hausdorff space any point is closed, so that this condition is necessary. But since the diagonal $\Delta \subset G \times G$ is the inverse image of the identity under the continuous mapping $G \times G \to G$, $(a, b) \to ab^{-1}$, it is also sufficient. □

Corollary. *Every Lie group is a Hausdorff topological group.* □

In defining smooth groups the condition that mapping (2) should be smooth is in fact unnecessary:

Proposition 1. *If for a group G, which is at the same time a smooth manifold, mapping* (1) *is smooth, then so is mapping* (2) *and hence the group G is a Lie group.*

Notice that for topological groups a similar statement is false.

A key to the proof of Proposition 1 is the following lemma from the theory of smooth manifolds:

Lemma 2. *Let M, N and R be smooth manifolds and let*

$$\varphi: M \times R \to N$$

be a smooth mapping such that for any point $r \in R$ the mapping

$$\varphi_r: M \to N, \quad x \mapsto \varphi(x, r), \qquad x \in M,$$

is a diffeomorphism of M onto the manifold N. Then the mapping

$$\psi: N \times R \to M$$

defined by the formula

$$\psi(y, r) = \varphi_r^{-1}(y), \qquad y \in N, \ r \in R,$$

is a smooth mapping.

Proof. Let the mappings

$$\Phi: M \times R \to N \times R, \ \Psi: N \times R \to M \times R$$

be defined respectively by the formulas

$$\Phi(x, r) = (\varphi(x, r), r) = (\varphi_r(x), r), \qquad x \in M, \ r \in R,$$

$$\Psi(y, r) = (\psi(y, r), r) = (\varphi_r^{-1}(y), r), \qquad y \in N, \ r \in R.$$

It is clear that these mappings are smooth if and only if so are the mappings φ and ψ respectively. Thus, under the hypothesis the mapping Φ is smooth and it is necessary to prove that so is the mapping Ψ.

To this end we notice that by definition

$$(\Psi \circ \Phi)(x, r) = \Psi(\varphi_r(x), r) = (\varphi_r^{-1}(\varphi_r(x)), r) = (x, r)$$

for any point $(x, r) \in M \times R$ and similarly

$$(\Phi \circ \Psi)(y, r) = \Phi(\varphi_r^{-1}(y), \quad r) = (\varphi_r(\varphi_r^{-1}(y)), r) = (y, r)$$

for any point $(y, r) \in N \times R$. This means that the mappings Φ and Ψ are inverse to each other and hence both are bijective mappings.

The statement about the smoothness of Ψ therefore is equivalent to the statement that the smooth bijective mapping Φ is a diffeomorphism.

But it is clear that a smooth bijective mapping is a diffeomorphism if and only if it is a local diffeomorphism, i.e. is

an étal mapping (i.e. at each point its differential is an isomorphism).

Everything has thus boiled down to calculating at each point $(a, r) \in M \times R$ the differential $(d\Phi)_{(a,r)}$ of the mapping Φ which may be regarded as a linear mapping of the form*.

(3) $\mathsf{T}_a(M) \oplus \mathsf{T}_r(R) \to \mathsf{T}_b(N) \oplus \mathsf{T}_r(R)$, where $b = \varphi(a, r)$.

Graphically every mapping (3) is given by a matrix of the form

(4) $$\begin{pmatrix} A & B \\ C & D \end{pmatrix}, \qquad \text{where}$$

$$A\colon \mathsf{T}_a(M) \to \mathsf{T}_b(N), \quad B\colon \mathsf{T}_r(R) \to \mathsf{T}_b(N),$$
$$C\colon \mathsf{T}_a(M) \to \mathsf{T}_r(R), \quad D\colon \mathsf{T}_r(R) \to \mathsf{T}_r(R)$$

are linear mappings defined in an obvious way. In particular, for the mapping $(d\Phi)_{(a,r)}$ the mapping A is nothing but the differential at a point a of the mapping $\varphi_r : M \to N$, the mapping C is the differential of the constant mapping (and consequently it is a zero mapping) and the mapping D is the differential of the identity mapping (and hence it is also an identity mapping). Thus for the differential $(d\Phi_{(a,r)}$ matrix (4) is of the form

$$\begin{pmatrix} (d\varphi_r)_a & B \\ 0 & \mathrm{id} \end{pmatrix}$$

(the mapping B is of no concern to us). Since the differential $(d\varphi_r)_a$ is an isomorphism by the hypothesis of the lemma, it follows that the differential $(d\Phi)_{(a,r)}$ is also an isomorphism. □

For every group G any element $a \in G$ defines by the formulas

$$L_a x = ax, \qquad R_a x = xa, \qquad x \in G$$

two mappings

$$L_a\colon G \to G, \qquad R_a : G \to G$$

---

* By $\mathsf{T}_x(M)$ we denote the tangent space to the manifold M at a point $x \in M$.

which are called *shifts by an element a* (the mapping L_a is called a *left shift* and the mapping R_a a *right shift*).

The following properties of shifts are obvious:

$$L_e = R_e = \mathrm{id}, \text{ where } e \text{ is the identity of the group } G$$

(this is exactly the same as stating that e is an identity)

$$L_b \circ L_a = L_{ba}, \quad R_b \circ R_a = R_{ab}, \quad L_a \circ R_b = R_b \circ L_a$$

(each of these equations is equivalent to the associativity of multiplication in a group).

In particular (since $L_a \circ L_{a^{-1}} = L_{a^{-1}} \circ L_a = L_e = \mathrm{id}$ and $R_a \circ R_{a^{-1}} = R_{a^{-1}} \circ R_a = R_e = \mathrm{id}$), we see that every shift is a bijective mapping, with

$$L_a^{-1} = L_{a^{-1}}, \qquad R_a^{-1} = R_{a^{-1}}$$

for any element $a \in G$.

If G is a topological (smooth) group, then the mappings L_a and R_a are continuous (smooth) and therefore they are homeomorphisms (diffeomorphisms).

Now we are in a position to prove Proposition 1.

Proof of Proposition 1. The smoothness of mapping (1) implies the smoothness of shifts L_a and hence the fact that they are diffeomorphisms. The corresponding mapping $L: (x, a) \mapsto L_a(x) = ax$ is nothing but mapping (1) and is therefore smooth. We are thus under the hypotheses of Lemma 1 (for $M = N = R = G$) and consequently by that lemma the mapping

$$L' : G \times G \to G$$

defined by the formula

$$L'(x, a) = L_a^{-1}(x) = a^{-1}x$$

is smooth. To complete the proof it remains to notice that the mapping $a \mapsto a^{-1}$ is the composition of the smooth mapping $G \to G \times G$, $a \mapsto (e, a)$, and of the mapping L'. Therefore it is also smooth. $\square$

Examples of Lie groups.

Example 1. Any abstract (discrete topological) group is a Lie group as a zero-dimensional smooth manifold.

Example 2. Any finite-dimensional vector space is a Lie group under addition.

Example 3. A unit circle $S^1 : |z| = 1$ whose points are complex numbers $z = e^{i\theta}$ is a Lie group under multiplication.

A Lie group under multiplication is similarly a *unit sphere* S^3 in the space of quaternions whose points are quaternions ζ for which $|\zeta| = 1$.

We can show that if a sphere S^n is a Lie group, then it is necessary that $n = 1$ or $n = 3$, so that S^1 and S^3 are the only spheres admitting the structure of a Lie group.

Example 4. The direct product $G \times H$ of two smooth (or topological) groups G and H is a smooth (respectively, topological) group.

In particular, any torus T^n, $n \geqslant 1$, is a Lie group.

Example 5. A full linear group $GL(n)$ is a Lie group. The group Aut $\mathscr{V}$ of all automorphisms (nonsingular linear operators) of an arbitrary n-dimensional vector space $\mathscr{V}$, which is isomorphic to the group $GL(n)$ is also a Lie group.

To obtain more interesting examples, it is first necessary to consider one general construction.

Definition 2. An $n \times n$ matrix A is said to be *nonexceptional* if $\det(E + A) \neq 0$. For such a matrix there is a matrix

$$A^{\#} = (E - A)(E + A)^{-1}$$

called the *Cayley image* of A.

It is clear that the set $\mathbb{R}(n)^0$ of all nonexceptional matrices is open in the manifold $\mathbb{R}(n) = \mathbb{R}(n, n)$ of all square $n \times n$ matrices and that hence it is a smooth manifold.

Proposition 2. *The mapping $A \mapsto A^{\#}$ is the involutory autodiffeomorphism of the manifold* $\mathbb{R}(n)^0$, i.e. *for any nonexceptional matrix A the matrix $A^{\#}$ is also nonexceptional, the mapping $A \mapsto A^{\#}$ of the manifold $\mathbb{R}(n)^0$ into itself is smooth and the Cayley image of $A^{\#}$ coincides with A*:

$$A^{\#\#} = A.$$

Proof. Let $B = A^{\#}$. Then

$$\begin{aligned} E + B &= E + (E - A)(E + A)^{-1} \\ &= [(E + A) + (E - A)](E + A)^{-1} \\ &= 2(E + A)^{-1} \end{aligned}$$

and similarly

$$E - B = 2A\,(E + A)^{-1}.$$

Therefore, firstly, $\det\,(E + B) \neq 0$ and secondly

$$B^{\#} = (E - B)\,(E + B)^{-1} = A.$$

It is obvious that the mapping $A \mapsto A^{\#}$ is smooth. □

Further examples of Lie groups.

Example 6. Suppose as ever that $\mathrm{O}(n)$ is the group of all orthogonal $n \times n$ matrices. We show that in the group $\mathrm{O}(n)$ the smoothness is naturally defined with respect to which $\mathrm{O}\,(n)$ is a Lie group.

Let A be a nonexceptional orthogonal matrix and let $B = A^{\#}$. Then $A^{\top} = A^{-1}$ and therefore, by the well-known rules of handling the transposed matrices,

$$\begin{aligned} B^{\top} &= (E + A^{\top})^{-1}(E - A^{\top}) = (E + A^{-1})^{-1}(E - A^{-1}) \\ &= (E + A^{-1})^{-1}A^{-1}\,A\,(E - A^{-1}) \\ &= (A\,(E + A^{-1}))^{-1}\,(A - E) \\ &= (A + E)^{-1}(A - E) = -\,(E - A)\,(E + A)^{-1} = -\,B. \end{aligned}$$

Conversely, if $B^{\top} = -\,B$, then

$$\begin{aligned} A^{\top} &= (E + B^{\top})^{-1}\,(E - B^{\top}) = (E - B)^{-1}\,(E + B) \\ &= (E + B)\,(E - B)^{-1} = A^{-1} \end{aligned}$$

and consequently A is an orthogonal matrix. We thus see that a *nonexceptional matrix is orthogonal if and only if its Cayley image is a skew-symmetric matrix.*

Since skew-symmetric matrices form a vector space $\left(\text{of dimension } \frac{n\,(n-1)}{2}\right)$ it follows that the mapping $A \mapsto A^{\#}$ may be considered as a coordinate function (mapping); the collection $\mathrm{O}\,(n)^0$ of all orthogonal nonexceptional matrices (which obviously contains a unit matrix E) is the corresponding coordinate neighbourhood and its image is the collection of all skew-symmetric nonexceptional matrices.

Now let C be an arbitrary orthogonal matrix. The set $\mathrm{O}\,(n)^0\,C$ consisting of all matrices of the form AC, where $A \in \mathrm{O}\,(n)^0$, contains the matrix C and is its neighbourhood. But the mapping $AC \mapsto A^{\#}$ is a coordinate mapping of that

neighbourhood onto an open set of nonexceptional skew-symmetric $n \times n$ matrices. Thus the entire group $\mathrm{O}(n)$ turns out to be covered with charts of the form $\mathrm{O}(n)^0 C$. If, however, $A_1C_1 = A_2C_2$, where $A_1, A_2 \in \mathrm{O}(n)^0$, and C_1 and C_2 are fixed matrices, then $A_2^{\#} = f(A_1^{\#})$, where f is some rational matrix function dependent on C_1 and C_2. The explicit expression for f can be written out without difficulty, but it is not necessary since (for our purposes) it is sufficient to make an obvious remark that each element of the matrix $A^{\#}$ is a rational and hence a smooth function of the elements of the matrix $A_1^{\#}$. It follows from this remark that any two charts of the form $\mathrm{O}(n)^0 C$ are compatible with each other and hence they all make an atlas. Since the Cayley image of the product of two matrices is obviously a rational function of the Cayley images of the factors, the corresponding smoothness on $\mathrm{O}(n)$ is compatible with multiplication, i.e. the *group* $\mathrm{O}(n)$ *provided with that smoothness is a Lie group.*

The trick with Cayley images is easily seen to have a very general character. Indeed, throughout the foregoing the specific character of orthogonal matrices was manifested only in that the Cayley images of nonexceptional orthogonal matrices constitute an open set of a vector space. A *matrix group*, therefore, *will be a Lie group if the Cayley images of its nonexceptional matrices constitute an open set of some vector space of matrices.*

Matrix groups having this property will be said to *admit a Cayley construction*, and the corresponding vector space of matrices will be called the *Cayley image* of a group.

Example 7. A matrix

$$\begin{pmatrix} A_1 & A_2 \\ A_3 & A_4 \end{pmatrix}$$

of even order $n = 2m$ is said to be a *symplectic matrix* if:

(a) $A_1^{\top}A_3$ and $A_2^{\top}A_4$ are symmetric matrices, and
(b) $A_1^{\top}A_4 - A_3^{\top}A_2 = E$.

These conditions are equivalent to a single matrix equation

$$A^{\top}JA = J, \tag{5}$$

where

$$J=\begin{pmatrix} 0 & E \\ -E & 0 \end{pmatrix}. \tag{6}$$

The symplecticity of the matrix implies that it preserves the bilinear skew-symmetric form

$$(x_1y_{n+1} - x_{n+1}y_1) + \ldots + (x_ny_{2n} - x_{2n}y_n).$$

In a more general way we can consider matrices A satisfying relation (5) for an arbitrary (but fixed) matrix J. When $J = E$ we obtain orthogonal matrices ($A^{\mathsf{T}}A = E$) and for this reason matrices A satisfyng (5) for a given matrix J are called *J-orthogonal matrices.* Thus symplectic matrices are J-orthogonal matrices corresponding to a matrix J of the form (6).

The relation

$$(AB)^{\mathsf{T}}\, J\, (AB) = B^{\mathsf{T}}\, (A^{\mathsf{T}}JA)\, B$$

directly implies that the product of two J-orthogonal matrices is a J-orthogonal matrix. If J is nonsingular, then passing in (5) to the determinants we at once see that $\det A = \pm 1$ and in particular that any J-orthogonal matrix is invertible. In view of the equation

$$(A^{-1})^{\mathsf{T}}JA^{-1} = (A^{-1})^{\mathsf{T}}(A^{\mathsf{T}}JA)\, A^{-1} = J$$

the inverse matrix A^{-1} is also a J-orthogonal matrix. This proves that *if J is a nonsingular matrix, all J-orthogonal matrices form a group.* In particular, symplectic matrices form a group.

We shall denote the group of J-orthogonal matrices of order n by $O_J(n)$ and the group of symplectic matrices of order $n = 2m$ by $\mathrm{Sp}(m; \mathbb{R})$.

The group $\mathrm{Sp}(m, \mathbb{R})$ is called a *real linear symplectic group.*

It is easy to see that *a nonexceptional matrix A is J-orthogonal if and only if its Cayley image $A^{\#}$ is a J-skew-symmetric matrix*, i. e. if

$$(A^{\#})^{\mathsf{T}}J = -JA^{\#}. \tag{7}$$

Indeed, if (5) holds, then

$$\begin{aligned}(A^{\#})^{\mathsf{T}}J &= (E + A^{\mathsf{T}})^{-1}(E - A^{\mathsf{T}})J \\ &= (E + JA)^{-1}J^{-1})^{-1}(E - JA^{-1}J^{-1})J \\ &= J(A^{-1}A + A^{-1})^{-1}(A^{-1}A - A^{-1}) \\ &= J(A + E)^{-1}(A - E) = -JA^{\#}.\end{aligned}$$

Conversely, it follows from (7) (assuming $B = A^{\#}$ and using the relation $B^{\#} = A$) that

$$\begin{aligned}A^{\mathsf{T}}JA &= (E + B^{\mathsf{T}})^{-1}(E - B^{\mathsf{T}})J\cdot(E - B)(E + B)^{-1} \\ &= (E + B^{\mathsf{T}})^{-1}\cdot J(E+B)\cdot(E+B)^{-1}(E - B) \\ &= (E+B^{\mathsf{T}})^{-1}\cdot J(E-B) = (E+B^{\mathsf{T}})^{-1}\cdot(E+B^{\mathsf{T}})J \\ &= J. \quad \square\end{aligned}$$

Since condition (7) is linear and hence defines a vector subspace in the space of all matrices, this proves that *every group* $\mathrm{O}_J(n)$ (and, in particular, the group $\mathrm{Sp}(m, \mathbb{R})$) *admits the Cayley construction and is therefore a Lie group.*

Since, as is easily seen, the vector space of matrices which is defined by condition (7) (with a matrix J given by formula (6)) has dimension $m(2m + 1)$, we deduce in particular that $\mathrm{Sp}(m; \mathbb{R})$ *is of dimension* $m(2m + 1)$.

Example 8. The intersection $\mathrm{Sp}(m; \mathbb{R}) \cap \mathrm{O}(2m)$ is called an *orthogonal symplectic group*. The Cayley images of nonexceptional matrices of this group are of the form

$$\begin{pmatrix} C & D \\ -D & C \end{pmatrix}, \tag{8}$$

where D is a symmetric matrix and C is a skew-symmetric matrix. Since matrices of the form (8) also constitute a vector space, $\mathrm{Sp}(m; \mathbb{R}) \cap \mathrm{O}(2m)$ *is a Lie group*. Its dimension is m^2.

Example 9. A Lie group can be constructed not only of real matrices but also of complex ones. For any $n \geqslant 1$, the complex vector space $\mathbb{C}^n$ can be identified with the space $\mathbb{R}^{2n}$ by writing out real and imaginary parts of the vector components in $\mathbb{C}^n$ in a fixed order. This defines in $\mathbb{C}^n$ (and hence in its any open subset) a structure of a smooth manifold of dimension $2n$ (independent, of course, of the order of writing out the real and imaginary parts of vector components in $\mathbb{C}^n$).

The set $\mathbb{C}(n, m)$ of all complex $n \times m$ matrices can be identified with $\mathbb{C}^{nm}$ and is also found to be a smooth manifold. A subset $\mathrm{GL}(n; \mathbb{C})$ of the set $\mathbb{C}(n) = \mathbb{C}(n, n)$ consisting of nonsingular matrices is also a smooth manifold. Since the real and imaginary parts of the elements of the product of two complex matrices are smooth functions of the real and imaginary parts of the elements of the factors, the manifold $\mathrm{GL}(n; \mathbb{C})$ is a Lie group (of dimension $2n^2$).

The concept of Cayley image with all its properties is directly extended to the complex case. The same applies to J-orthogonal matrices. In particular, we thus obtain *complex orthogonal* and *complex symplectic matrices*. They constitute the Lie group $\mathrm{O}(n; \mathbb{C})$ and $\mathrm{Sp}(m; \mathbb{C})$ of dimension $n(n-1)$ and $2m(m+1)$ respectively.

Example 10. Of quite another type of complex matrices are *J-unitary matrices A* of order n which are characterized by the relation

$$\bar{A}^{\mathsf{T}} JA = J.$$

They make a group $\mathrm{U}_J(n)$. When $J = E$ we obtain usual *unitary matrices* and their group $\mathrm{U}(n)$. When J is a matrix (6), (and $n = 2m$) the group $\mathrm{U}_J(n)$ has no generally accepted notation. We shall denote it by $\mathrm{Up}(m)$.

By essentially the same calculations as earlier, we can easily prove that a *nonexceptional complex matrix A is J-unitary if and only if its Cayley image $A^{\#}$ satisfies the relation*

$$(\bar{A}^{\#})^{\mathsf{T}} J = -JA^{\#}. \ \square$$

Since this relation is linear (over the field $\mathbb{R}$ the *group* $\mathrm{U}_J(n)$ *(and,* $\mathrm{U}(n)$ *and* $\mathrm{Up}(m)$, *in particular) is a Lie group*. $\square$

The group $\mathrm{U}(n)$ is of dimension n^2, and $\mathrm{Up}(m)$ is of dimension $4m^2$.

Notice that $\mathrm{U}(n)$ *is naturally isomorphic to the orthogonal symplectic group* $\mathrm{Sp}(n; \mathbb{R}) \cap \mathrm{O}(2n)$. The isomorphism is realized by the correspondence

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} \mapsto A + iB.$$

The intersection of $\mathrm{U}(2m)$ and $\mathrm{Sp}(m; \mathbb{R})$ is obviously an

orthogonal symplectic group:

$$\mathrm{Sp}\,(m,\ \mathbb{R}) \cap \mathrm{U}\,(2m) = \mathrm{Sp}\,(m;\ \mathbb{R}) \cap \mathrm{O}\,(2m)$$

(and so it is isomorphic to $\mathrm{U}\,(m)$).

Example 11. The intersection $\mathrm{Sp}\,(m;\ \mathbb{C}) \cap \mathrm{U}\,(2m)$ is called a *unitary symplectic group* (or simply a *symplectic group*) and denoted by $\mathrm{Sp}\,(m)$. It is a Lie group of dimension $m\,(2m+1)$.

The intersection of $\mathrm{Sp}\,(m)$ and $\mathrm{O}\,(2m)$ is an orthogonal symplectic group $\mathrm{Sp}\,(m) \cap \mathrm{O}\,(2m)$.

Example 12. The group $\mathrm{U}\,(m)$ may be interpreted as a group of all invertible linear transformations of $\mathbb{C}^n$ space which preserve the Hermitian form $x_1\bar{y}_1 + \ldots + x_n\bar{y}_n$. Similarly, by replacing the field $\mathbb{C}$ by the quaternion field $\mathbb{H}$ we can introduce the group $\mathrm{U}^{\mathbb{H}}\,(n)$ of all invertible and linear (with respect to, say, premultiplication) transformations of the quaternion space $\mathbb{H}^n$ which preserve the quaternion Hermitian form

$$(\xi,\ \eta) = \xi_1\,\bar{\eta}_1 + \ldots + \xi_n\bar{\eta}_n,$$

where $\xi = (\xi_1,\ \ldots,\ \xi_n) \in \mathbb{H}^n$, $\eta = (\eta_1,\ \ldots,\ \eta_n) \in \mathbb{H}^n$.

Since any quaternion ξ can be identified with a pair $(u,\ v)$ of complex numbers (by the formula $\xi = u + vj$) and hence the space $\mathbb{H}^n$ with the space $\mathbb{C}^{2n}$, the group $\mathrm{U}^{\mathbb{H}}\,(n)$ is naturally interpreted as a group of complex matrices. If

$$\xi_1 = x_1 + x_{n+1}j,\ \ldots,\qquad \xi_n = x_n + x_{2n}j,$$

$$\eta_1 = y_1 + y_{n+1}j,\ \ldots,\qquad \eta_n = y_n + y_{2n}j,$$

then (since $\overline{u+vj} = \bar{u} - vj$ and $vj = j\bar{v}$)

$$\begin{aligned}\xi_1\bar{\eta}_1 + \ldots\quad & \xi_n\bar{\eta}_n \\ &= [x_1\bar{y}_1 + \ldots + x_n\bar{y}_n + x_{n+1}\bar{y}_{n+1} + \ldots + x_{2n}\bar{y}_{2n}] \\ &\qquad + [(x_{n+1}y_1 - x_1y_{n+1}) + \ldots + (x_{2n}y_n - x_ny_{2n})]j.\end{aligned}$$

Therefore, every element of $\mathrm{U}^{\mathbb{H}}\,(n)$ interpreted as a complex matrix preserves the Hermitian form $x_1\bar{y}_1 + \ldots + x_{2n}\bar{y}_{2n}$ (is a unitary matrix) and the skew-symmetric form $(x_{n+1}y_1 - x_1y_{n+1}) + \ldots + (x_{2n}y_n - x_ny_{2n})$ (is a symplectic matrix), i.e. it is in the unitary symplectic group $\mathrm{Sp}\,(n)$. Conversely, if a matrix A is unitary and symplectic,

then, if interpreted as a transformation of the space $\mathbb{H}^n$, it obviously preserves the form $\xi_1, \bar{\eta}_1 + \ldots + \xi_n\bar{\eta}_n$. Moreover, this transformation is linear. Indeed, it obviously turns a sum into a sum, so that it is only necessary to prove that it commutes with the operation of multiplication by an arbitrary quaternion ζ. But for any vectors $\xi = (\xi_1, \ldots, \xi_n) \in \mathbb{H}^n$ and $\eta = (\eta_1, \ldots, \eta_n) \in \mathbb{H}^n$ we have

$$\begin{aligned}(A(\zeta\xi) - \zeta A\xi, A\eta) &= (A(\zeta\xi), A\eta) - \zeta(A\xi, A\eta)\\ &= (\zeta\xi, \eta) - \zeta(\xi, \eta) = 0,\end{aligned}$$

from which it follows (since any vector in $\mathbb{H}^n$ can be represented in the form $A\eta$) that $A(\zeta\xi) = \zeta A\xi$.

This proves that the group $U^{\mathbb{H}}(n)$ *is isomorphic to the unitary symplectic group* $\mathrm{Sp}(n)$. □

Recall that a topological space X is said to be *connected*, if it cannot be represented as a union of two nonempty disjoint and closed (open) sets, and *arcwise connected*, if for any points $a, b \in X$ there is a *path* that joins them, i.e. a continuous mapping $u: [0, 1] \to X$ such that $u(0) = a$, $u(1) = b$. It is intuitively obvious (and easy to prove within the framework of any rigorous theory of real numbers) that the *interval* $[0, 1]$ *is connected* from which it immediately follows that *any arcwise connected space is connected*.

It is obvious that the set of all (arcwise) connected subsets of an arbitrary topological space X is inductive (satisfies the hypothesis of Zorn's lemma). Therefore every point $a \in X$ is contained in the maximal connected subset C_a called a *component of (arcwise) connectedness of* X. It is easy to see that any component of connectedness $C_a \subset X$ is closed in X (but not open in general). The space X is (arcwise) connected if and only if $C_a = X$ for any point $a \in X$.

The topological space X is said to be *locally (arcwise) connected* if every point $a \in X$ has a fundamental system of (arcwise) connected neighbourhoods, i.e. in other words, if every neighbourhood of a contains a (arcwise) connected neighbourhood. An example of a locally arcwise connected space is an arbitrary manifold.

In a locally (arcwise) connected space any component of

(arcwise) connectedness is obviously open (for together with every point it contains a certain neighbourhood of it). In particular, it follows that if a *space is connected and locally arcwise connected, it is also connected.* In other words, for locally arcwise connected spaces (in particular, for manifolds) the concepts of connectedness and arcwise connectedness coincide.

Example 13. The manifolds $\mathbb{R}^n$ and $\mathbb{R}(n, m)$ are, obviously, connected. The manifold GL (n) is not connected: no matrix with a negative determinant can be continuously deformed (connected by a path) into a unit matrix. Let $\mathrm{GL}^+(n)$ be the space of all square $n \times n$ matrices with a positive determinant. We show that the *space* $\mathrm{GL}^+(n)$ *is connected.*

By the theorem on polar factorization (see II, 21) any nonsingular operator is the product of a positive operator P and an isometric (orthogonal) operator U. In matrix terms this implies that any nonsingular matrix A is of the form $A = PU$, where P is the matrix of the positive operator and U is an orthogonal matrix. On the other hand, by the theorem on the reduction to the principal axes the matrix P is of the form VDV^{-1}, where V is an orthogonal matrix and D is a diagonal matrix with positive diagonal elements. Hence $A = VDV^{-1}U$, i.e. $A = VDW$, where $W = V^{-1}U$. But it is clear that the correspondence $t \mapsto (1 - t) D + tE$ is a continuous path in GL (n) connecting D with a unit matrix E. By multiplying that path from the right and from the left by the orthogonal matrices V and W we obtain a continuous path joining in GL (n) the matrix A to the orthogonal matrix $B = VW$. Thus *any nonsingular matrix* A *can be joined to the orthogonal matrix* B *by a continuous path in* GL (n). If $\det A > 0$, then $\det B > 0$, i.e. $\det B = 1$ (an orthogonal matrix with a positive determinant is unimodular). To prove that the group $\mathrm{GL}^+(n)$ is connected, therefore, it suffices to verify that *any unimodular orthogonal matrix* B *can be joined to a unit matrix* E *by a continuous path* (in $\mathrm{GL}^+(n)$). We prove even more, namely that *this joining can be realized in the group* SO (n) *of all unimodular orthogonal matrices.* To this end notice that according to the fundamental theorem on orthogonal operators (see II, 21) every unimodular (i.e. orientation-preserving) orthogonal operator (rotation) is the direct sum of an identity operator and

"two-dimensional rotations" with matrices of the form

$$\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}.$$

By replacing in each of these matrices the angle θ by $t\theta$ we obtain a continuous family (path) of orthogonal operators which joins a given operator (resulting when $t = 1$) to the identity operator (resulting when $t = 0$). To complete the proof we have to pass from operators to matrices. □

The established statement implies that the *group* GL (n) *consists of two components*: the subgroup $\mathrm{GL}^+(n)$ and its coset $\mathrm{GL}^-(n)$ consisting of matrices with negative determinants.

For every topological group G we shall use the symbol G_e to denote the component of its identity e. If $a \in G_e$, then $a \in L_a(G_e)$ (since $e \in G_e$) and hence $G_e \cap L_a(G_e) \neq \varnothing$. Therefore in view of the connectedness and maximality of G_e, and hence of $L_a(G_e)$, we have $L_a(G_e) = G_e$. It can be proved in a similar way that $R_a(G_e) = G_e$ if $a \in G_e$ and that $G_e^{-1} = G_e$. This means that G_e is a subgroup of group G. Moreover, any endomorphism T of G turns G_e into a connected subgroup $T(G_e)$ which intersects G_e. By the same considerations, therefore, $T(G_e) \subset G_e$. This means that the *component of identity G_e is a completely characteristic subgroup of G and is, in particular, invariant.*

According to the foregoing the component of identity of the group GL (n) is the group $\mathrm{GL}^+(n)$.

Notice that for every smooth group G the component G_e is automatically a smooth group.

It is natural to introduce into the factor group G/G_e a topology of identificaion, i.e. a topology in which the subset $C \subset G/G_e$ is open (closed) if and only if so is its complete inverse image in G. Since the inverse image of the identity of G/G_e is the component G_e, we see in particular that the identity of the factor group G/G_e is isolated (is both an open and closed set), in other words G/G_e is discrete, if and only if G_e is open (it is always closed). In particular, this is clearly so if the group G is locally connected (if it is a smooth group, for example).

Thus *any locally connected* (*in particular*, *any smooth*) *group*

G is an extension of a connected group (of its component of identity G_e) by means of the discrete group G/G_e.

In this sense the theory of any locally connected groups reduces to the theory of connected groups and to the theory of discrete (abstract) groups.

For this reason in the general theory we shall always assume all Lie groups under consideration to be connected.

Example 14. According to the foregoing SO (n) is a *connected group* and hence the component of identity of the group O (n). In particular, we see that SO (n) *is a Lie group.*

At the same time we see that O (n) *is not connected* and consists of two components: the group SO (n) = O^+ (n) of proper (unimodular) orthogonal matrices and its coset O^- (n) whose elements are improper (with determinant —1) orthogonal matrices.

Example 15. On the contrary, U (n) *is a connected group.* Indeed, we know (see II, 21) that any unitary operator is orthogonally diagonalizable, all its eigenvalues equaling unity in absolute value. In matrix terms this means that any unitary matrix is of the form UDU^{-1}, where U is some unitary matrix and D is a diagonal matrix with diagonal elements of the form $e^{i\theta_k}$. By replacing all angles θ_k by $t\theta_k$ we obtain a continuous family (path) of unitary matrices which joins a given matrix resulting when $t = 1$ to a unit matrix resulting when $t = 0$. (For orthogonal matrices see the above reasoning). □

That U (n) is a connected group can be proved in a different way, using the following general lemma:

Lemma 3. *A topological group G is connected if it contains a connected subgroup H with a connected factor space G/H.*

Proof. Notice first that a *natural mapping* $\pi: G \to G/H$ *is open*, i.e. it turns open sets into open sets. Indeed, if $U \subset G$, then by definition of factor topology a set $\pi(U) \subset G/H$ is open if and only if so is $\pi^{-1}(\pi(U)) \subset G$. But it is clear that the latter is the union $\bigcup_{x \in U} xH$ of all cosets xH, $x \in U$, and hence coincides with the union $\bigcup_{h \in H} Uh$ of all shifts of U by the elements $h \in H$. Therefore, if U and hence any Uh is open, then the set $\pi^{-1}(\pi(U))$ and hence $\pi(U)$ are open.

Now let $G = U \cup V$, where U and V are nonempty sets. Then $G/H = \pi(U) \cup \pi(V)$, where $\pi(U)$ and $\pi(V)$ are also nonempty and open. Therefore, $\pi(U) \cap \pi(V) \neq \varnothing$ is nonempty either (since the space G/H is assumed to be connected). Let $\pi(a) \in \pi(U) \cap \pi(V)$. The inclusion $\pi(a) \in \pi(U)$ implies that the coset $\pi(a) = aH$ intersects U and the inclusion $\pi(a) \in \pi(V)$ implies that the coset intersects V. We have, $aH = U_1 \cap V_1$, where $U_1 = aH \cap U$ and $V_1 = aH \cap V$ are open in aH (and nonempty according to the foregoing). Since aH (together with H) is connected, this is possible if and only if $U_1 \cap V_1 \neq \varnothing$ and hence $U \cap V \neq \varnothing$. Consequently G is connected. □

To apply the lemma we consider a mapping $\mathrm{U}(n) \to \mathbb{C}^n$ which associates the last column with every matrix. The image of $\mathrm{U}(n)$ under the mapping consists of all vectors of space $\mathbb{C}^n$ of length 1 and hence can be identified with a unit $(2n-1)$-dimensional sphere S^{2n-1} of $\mathbb{R}^{2n} = \mathbb{C}^n$. The inverse image of every such vector in $\mathrm{U}(n)$ is obviously a coset relative to the subgroup $\mathrm{U}(n-1)$ which is the inverse image of the vector $(0, 0, \ldots, 0, 1)$. Consequently, the mapping in question induces a bijective mapping $\mathrm{U}(n)/\mathrm{U}(n-1) \to S^{2n-1}$ of the factor space $\mathrm{U}(n)/\mathrm{U}(n-1)$ onto S^{2n-1} which is easily verified to be a homeomorphism.

Since $S^{2n-1} = \mathrm{U}(n)/\mathrm{U}(n-1)$ is in an obvious way connected, it immediately follows from Lemma 2 that $\mathrm{U}(n)$ is connected if so is $\mathrm{U}(n-1)$. Since $\mathrm{U}(1)$ is in a natural way identified with the group S^1 and is therefore connected, the connectedness of all groups $\mathrm{U}(n)$ is found, by induction, to be proved anew.

Example 16. A similar reasoning applies also to the symplectic group $\mathrm{Sp}(n) = \mathrm{U}^{\mathbb{H}}(n)$. In this case the factor space $\mathrm{Sp}(n)/\mathrm{Sp}(n-1)$ is identified in a natural way with a unit sphere S^{4n-1} of $\mathbb{R}^{4n} = \mathbb{H}^n$ and hence it is also connected. But $\mathrm{Sp}(1) = \mathrm{U}^{\mathbb{H}}(1)$ is identified with the group S^3 of quaternions ξ for which $|\xi| = 1$. Consequently *for any* $n \geqslant 1$ *the group* $\mathrm{Sp}(n) = \mathrm{U}^{\mathbb{H}}(n)$ *is connected.*

The same reasoning can also be applied to the group $\mathrm{SO}(n)$ whose connectedness we have established earlier on the basis of other considerations. Indeed, in this case $\mathrm{SO}(n)/\mathrm{SO}(n-1)$ is identified in the same way with a unit sphere S^{n-1} of $\mathbb{R}^n$ which, for $n \geqslant 2$, is connected.

Moreover, SO (2), the group of rotations of a plane, is known to be isomorphic to the group $\mathbb{S}^1$ and hence it is also connected. *For* $n \geqslant 2$, *therefore*, SO (n) *is connected.*

The analogue of SO (n) in U (n) is the *subgroup* SU (n) of *unimodular unitary matrices.* Since, as is easily seen, SU (n)/SU $(n-1)$ = U (n) /U $(n-1)$ and, being a unit group, SU (1) is connected, the same reasoning shows that *for any* $n \geqslant 1$ *the group* SU (n) *is connected.* It will be possible to establish whether it is a Lie group, however, only in Lecture 3, after we have developed the necessary tools.

The same applies to the group SL (n) of all unimodular matrices.

Notice that there is no analogue of the group SU (n) for $\mathrm{U}^{\mathbb{H}}$ (n).

Lecture 2

Left-invariant vector fields·Parallelizability of Lie groups·Integral curves of left-invariant vector fields and one-parameter subgroups·Lie functor·An example: a group of invertible elements of an associative algebra·Functions with values in an associative algebra·One-parameter subgroups of the group $G(\mathcal{A})$

Recall that by $\mathsf{T}_a(M)$ we denote a tangent space to a manifold M at a point $a \in M$. All tangent spaces $\mathsf{T}_a(M)$, $a \in M$, constitute a smooth $2n$-dimensional ($n = \dim M$) manifold $\mathsf{T}(M)$ projecting in a natural way onto M. The projection

$$\pi: \mathsf{T}(M) \to M$$

associates the "point of application", i.e. a point $a \in M$ for which $A \in \mathsf{T}_a(M)$ with every vector A so that $\mathsf{T}_a(M) = \pi^{-1}(a)$. The sections of this projection, i.e. the smooth mappings

$$X: M \to \mathsf{T}(M), \qquad a \mapsto X_a, \qquad a \in M,$$

for which $\pi \circ X = \mathrm{id}$, i.e. $X_a \in \mathsf{T}_a(M)$, are called *vector fields on M*. These vector fields form in a natural way a linear (infinite-dimensional) space which will be denoted by $\mathfrak{a}(M)$.

Differentials $(d\Phi)_a: \mathsf{T}_a(M) \to \mathsf{T}_{\Phi a}(N)$ of an arbitrary smooth mapping $\Phi: M \to N$ constitute a smooth mapping $\mathsf{T}(\Phi): \mathsf{T}(M) \to \mathsf{T}(N)$ for which we have a commutative

diagram

$$\begin{tikzcd}
\mathsf{T}(M) \arrow[r, "\mathsf{T}(\Phi)"] \arrow[d, "\pi"'] & \mathsf{T}(N) \arrow[d, "\pi"] \\
M \arrow[r, "\Phi"'] & N
\end{tikzcd}$$

and the correspondences $M \mapsto \mathsf{T}(M)$ and $\Phi \mapsto \mathsf{T}(\Phi)$ are obviously a functor from the category DIFF of smooth manifolds into itself.

If Φ is a diffeomorphism, then for any vector field X in $\mathfrak{a}(M)$ a field

$$\Phi_* X = \mathsf{T}(\Phi) \circ X \circ \Phi^{-1}$$

from $\mathfrak{a}(N)$ is defined and for any vector field Y from $\mathfrak{a}(N)$ a field

$$\Phi^* Y = \mathsf{T}(\Phi)^{-1} \circ Y \circ \Phi$$

from $\mathfrak{a}(M)$ is defined. It is clear that the mappings Φ_* and Φ^* are linear, and since

$$\Phi_* = (\Phi^*)^{-1} = (\Phi^{-1})^* \text{ and } \Phi^* = (\Phi_*)^{-1} = (\Phi_*^{-1}),$$

they are reciprocal isomorphisms of vector spaces.

If, in particular, $M = N = G$, where G is some Lie group, then for any element $a \in G$ and any vector field $X \in \mathfrak{a}(G)$ a vector field $L_a^* X \in \mathfrak{a}(G)$ is defined.

Definition 1. A field $X \in \mathfrak{a}(G)$ is said to be *left-invariant* if $L_a^* X = X$ for any element $a \in G$, i.e. if

(1) $\quad X_b = (dL_{a^{-1}})_{ab}(X_{ab})$ for any elements $a, b \in G$.

It is clear that all left-invariant fields form a subspace of the space $\mathfrak{a}(G)$ of all vector fields. We shall denote that subspace by $\mathfrak{l}(G)$ or $\mathfrak{g}$.

It is easily seen that a *field $X \in \mathfrak{a}(G)$ is left-invariant if and only if*

(2) $$X_a = (dL_a)_e X_e$$

for any element $a \in G$. Indeed, relation (2) is a special case (for $b = e$) of formula (1) and is therefore satisfied if X is left-invariant. Conversely, if (2) is satisfied, then for any elements $a, b \in G$

$$X_{ab} = (dL_{ab})_e (X_e) = ((dL_a)_b \circ (dL_b))_e(X_e) = (dL_a)_b(X_b),$$

which is equivalent to (1). □

It follows that the *linear mapping* $X \mapsto X_e$ *of* $\mathfrak{g}$ *into a tangent space* $\mathsf{T}_e(G)$ *is an isomorphism*. Indeed, for any vector $A \in \mathsf{T}_e(G)$ the mapping $a \mapsto (dL_a)_e A$, $a \in G$, is easily seen to be a vector field on G (it is only necessary to verify smoothness which can be at once discovered if we express the mapping in local coordinates) which has property (1) and hence is left-invariant. To complete the proof it remains to notice that the resulting mapping $\mathsf{T}_e(G) \mapsto \mathfrak{g}$ is obviously the inverse of the mapping $X \mapsto X_e$. □

As a rule, we shall use $X \mapsto X_e$ to identify $\mathfrak{g} = \mathfrak{l}(G)$ with $\mathsf{T}_e(G)$.

Since $\dim \mathsf{T}_e(G) = n$, where $n = \dim G$, we see, in particular, that *for any Lie group* G *the space* $\mathfrak{g} = \mathfrak{l}(G)$ *of left-invariant vector fields is finite-dimensional and is of dimension* $n = \dim G$.

Let $\mathcal{F}(M)$ be the algebra of all smooth functions on a smooth manifold M. For any function $f \in \mathcal{F}(M)$ and any field $X \in \mathfrak{a}(M)$ the formula

$$(fX)_a = f(a) X_a, \qquad a \in M,$$

obviously defines some field $fX \in \mathfrak{a}(M)$ and a straightforward verification shows that with respect to the operation $(f, X) \mapsto fX$ the vector space $\mathfrak{a}(M)$ turns out to be a module over $\mathcal{F}(M)$. If that module is a free module of rank n, i.e. if there is a system $X_1, \ldots, X_n$ of vector fields (a basis of the $\mathcal{F}(M)$-module $\mathfrak{a}(M)$) on M such that any field $X \in \mathfrak{a}(M)$ is uniquely represented as

$$X = f^1 X_1 + \ldots + f^n X_n,$$

where $f^1, \ldots, f^n \in \mathcal{F}(M)$, then the manifold M is said to be *parallelizable*.

Proposition 1. *Any Lie group* G *is parallelizable.*

Proof. We prove even more, namely that *every basis*

$X_1, \ldots, X_n$ *of a vector space* $\mathfrak{l}(G)$ *is a basis of the* $\mathscr{F}(M)$-*module* $\mathfrak{a}(G)$.

For every point $a \in G$, vectors $(X_1)_a, \ldots, (X_n)_a$ form a basis of a vector space $\mathsf{T}_a(G)$. Therefore, the vector X_a of an arbitrary vector field $X \in \mathfrak{a}(G)$ is uniquely expanded with respect to the vectors $(X_1)_a, \ldots, (X_n)_a$. This means that for every vector field $X \in \mathfrak{a}(G)$ there are functions $f^i : a \mapsto f^i(a)$, $a \in G$, such that $X = f^1X_1 + \ldots + f^nX_n$. It is only necessary therefore to prove that $f^k \in \mathscr{F}(G)$ for all $k = 1, \ldots, n$.

Let $(U, x^1, \ldots, x^n)$ be an arbitrary chart of the manifold G. Since the fields $X_1, \ldots, X_n$ are smooth, on U there are smooth functions $X_1^i, \ldots, X_n^i$, $i = 1, \ldots, n$, such that

$$X_j = X_j^i \frac{\partial}{\partial x^i} \text{ for any } j = 1, \ldots, n.$$

In addition, since for every point $a \in U$ vectors $(X_1)_a, \ldots, (X_n)_a$ form a basis of $\mathsf{T}_a(G)$, we have

$$\det(X_j^i) \neq 0 \quad \text{on} \quad U,$$

and therefore on U there are smooth functions Y_i^k such that

$$X_j^iY_i^k = \delta_j^k, \qquad i, j, k = 1, \ldots, n.$$

Under the hypothesis $X = f^jX_j$ and hence

$$X = f^jX_j^i \frac{\partial}{\partial x^i},$$

i.e. $f^jX_j^i$, $i = 1, \ldots, n$, are components of X in local coordinates $x^1, \ldots, x^n$ and are therefore smooth. But

$$f^k = f^j\delta_j^k = (f^jX_j^i)Y_i^k$$

and since $f^jX_j^i$ and Y_i^k are smooth so are (on U) f^k.

Being smooth functions on every coordinate neighbourhood U, functions f^k are smooth on the entire manifold G. □

Recall that a smooth curve $t \mapsto \varphi(t)$ on a manifold M is said to be an *integral curve* of a vector field if

$$\frac{d\varphi(t)}{dt} = X_{\varphi(t)} \quad \text{for any } t.$$

An integral curve is said to be *maximal* if it is not a restriction of an integral curve defined on a larger interval of the

real axis. It easily follows from the standard theorem on the existence and uniqueness of the solution of a system of differential equations with smooth right-hand sides and from elementary properties of Hausdorff spaces that if the manifold M is Hausdorff (which, as we know, is automatically satisfied for a Lie group), then *for any point* $a \in M$ *there exists a maximal integral curve* φ_a *of* X, *passing for* $t = 0$, *through point* a, *i.e. such that* $\varphi_a(0) = a$.

If for every point $a \in M$ the curve φ_a is defined on the entire axis $\mathbb{R}$ then the vector field X is said to be *complete.*

It is easy to see that a *vector field* X *on a Lie group* G *is left-invariant if and only if for any two points* $a, b \in G$

$$\varphi_{ab} = L_a \circ \varphi_b \tag{3}$$

i.e. $\varphi_{ab}(t) = a\varphi_b(t)$, $t \in \mathbb{R}$. Indeed, for any fixed $a \in G$ the formula $\psi_b(t) = \varphi_{a^{-1}b}(t)$ defines for any point $b \in G$ a certain curve $t \mapsto \psi_b(t)$ passing, for $t = 0$, through b and it is clear that by setting

$$Y_b = \left.\frac{d\psi_b(t)}{dt}\right|_{t=0}$$

we obtain on G a certain vector field $Y: b \mapsto Y_b$. By the rules for calculating tangent vectors to smooth curves, for any point $b \in G$, we have

$$\begin{aligned} Y_b &= \left.\frac{d\psi_b(t)}{dt}\right|_{t=0} = \left.\frac{d(L_a \circ \varphi_{a^{-1}b}(t))}{dt}\right|_{t=0} \\ &= (dL_a)_{a^{-1}b}\left(\left.\frac{d\varphi_{a^{-1}b}(t)}{dt}\right|_{t=0}\right) = (dL_a)_{a^{-1}b}(X_{a^{-1}b}). \end{aligned}$$

Therefore, if (3) is satisfied and consequently $\psi_b = \varphi_b$ (and hence $Y_b = X_b$), then $X_b = (dL_a)_{a^{-1}b}(X_{a^{-1}b})$ and in particular, $X_a = (dL_a)_e(X_e)$. Consequently the field X is left-invariant. Conversely, if X is left-invariant (and hence satisfies relation (1)), then $Y_b = X_b$, for any point $b \in G$, i.e. $Y = X$. But it is clear that $t \mapsto \psi_b(t)$ are integral curves of Y (which are automatically maximal) and therefore in view of the equation $Y = X$ these curves coincide with the integral curves $t \mapsto \varphi_b(t)$ of X. Thus $\varphi_b(t) = a\varphi_{a^{-1}b}(t)$, which is equivalent to (3). □

Definition 2. A smooth curve $\beta: \mathbb{R} \to G$ is said to be

a *one-parameter subgroup* of a Lie group G if

$$\beta(t+s) = \beta(t)\,\beta(s)$$

for any $t, s \in \mathbb{R}$. In other words, a one-parameter subgroup is a homomorphism of the additive group $\mathbb{R}$ of real numbers (which is treated as a Lie group) into the Lie group G.

It should be noted that a one-parameter subgroup is thus not a subset but a mapping.

It is obvious that for $t = 0$ every one-parameter subgroup β passes through the identity e of G:

$$\beta(0) = e.$$

Proposition 2. *Every one-parameter subgroup β is an integral curve of some left-invariant vector field X.*

Proof. The formula

$$\varphi_a(t) = a\beta(t), \qquad a \in G, \quad t \in \mathbb{R},$$

defines on G a smooth curve $t \mapsto \varphi_a(t)$ passing, for $t = 0$, through point a. We set

$$X_a = \left.\frac{d\varphi_a(t)}{dt}\right|_{t=0}.$$

A direct check shows that the mapping $a \mapsto X_a$ is smooth, i.e. is a vector field on G, and that curves φ_a are integral curves of that field. An integral curve is thus the curve $\varphi_e = \beta$. Finally, since

$$\varphi_{ab}(t) = (ab)\,\beta(t) = a\,(b\beta(t)) = a\varphi_b(t),$$

the field X is left-invariant. $\square$

The converse of Proposition 2 is also true:

Proposition 3. *A maximal integral curve β of a left-invariant vector field $X \in \mathfrak{g}$ which passes, for $t = 0$, through point e is a one-parameter subgroup of a Lie group G (and is, in particular, defined on the entire axis $\mathbb{R}$).*

Proof. Since X is left-invariant, its integral curves φ_a satisfy relation (3). Thus the interval I_a of the axis $\mathbb{R}$ on which an integral curve φ_a is defined, coincides with the interval $I = I_e$ on which an integral curve $\beta = \varphi_e$ is defined. Furthermore because for any fixed $s \in \mathbb{R}$ the curve $t \mapsto \varphi_e(t+s)$ is an integral curve of the field X, which passes through point $b = \varphi_e(s)$ and hence $\varphi_e(t+s) = \varphi_b(t)$,

we have

$$\begin{aligned}(4)\qquad \beta(s+t) &= \beta(t+s) = \varphi_e(t+s)\\ &= \varphi_b(t) = b\varphi_e(t) = \varphi_e(s)\,\varphi_e(t)\\ &= \beta(s)\,\beta(t)\end{aligned}$$

for any $s, t \in I$ such that $s + t \in I$. To prove Proposition 3 therefore, it is only necessary to show that β is defined on the entire axis $\mathbb{R}$, i.e. that $I = \mathbb{R}$.

Let $I \neq \mathbb{R}$. For any $t \in \mathbb{R}$ there is an integer n such that $\frac{t}{n} \in I$. We define the curve β for any $t \in \mathbb{R}$ by setting

$$\beta(t) = \beta\left(\frac{t}{n}\right)^n, \quad \text{if } \frac{t}{n} \in I.$$

This definition is correct. Indeed, if $\frac{t}{n} \in I$ and $\frac{t}{m} \in I$, then $\frac{t}{nm} \in I$ and hence, by relation (4),

$$\beta\left(\frac{t}{n}\right)^n = \left[\beta\left(\frac{t}{nm}\right)^m\right]^n = \left[\beta\left(\frac{t}{nm}\right)^n\right]^m = \beta\left(\frac{t}{m}\right)^m.$$

Thus the curve β is extended to the entire axis $\mathbb{R}$. It is clear that the curve thus constructed is smooth and satisfies relation (4) for all $t, s \in \mathbb{R}$, i.e. it is a one-parameter subgroup. Assuming $I \neq \mathbb{R}$ we arrive at a contradiction to the assumption if we show that the curve β on the entire axis $\mathbb{R}$ is an integral curve of the field X.

Let $t_0 \in \mathbb{R}$ and let $a = \beta(t_0)$. By definition the tangent vector $\frac{d\beta(t_0)}{dt}$ to β at point a acts on the functions* $f \in \mathcal{O}_a(G)$ according to the formula

$$\frac{d\beta(t_0)}{dt} f = \frac{d(f \circ \beta)(t)}{dt}\bigg|_{t=t_0}.$$

*For any smooth manifold M and any of its points a we denote by $\mathcal{O}_a(M)$ the set of all functions *smooth at point a*, i.e. defined in some, function-dependent, neighbourhood of a and smooth in the neighbourhood. (Strictly speaking, by $\mathcal{O}_a(M)$ we should understand a vector space of the germs of such functions, but we are not going to be over-strict.)

By $\mathcal{O}(M)$ we shall denote the set of all functions f defined and smooth in some, function-dependent, open set $W(f) \subset M$.

Similarly the tangent vector $\frac{d\beta(0)}{dt}$ at point e acts on the functions $f \in \mathcal{O}_e(G)$ according to the formula

$$\frac{d\beta(0)}{dt} f = \left.\frac{d(f \circ \beta)(t)}{dt}\right|_{t=0}.$$

Consequently, for any function $f \in \mathcal{O}_a(G)$

$$\left[(dL_a)_e \frac{d\beta(0)}{dt}\right] f = \frac{d\beta(0)}{dt}(f \circ L_a)$$

$$= \left.\frac{d(f \circ L_a \circ \beta)(t)}{dt}\right|_{t=0} = \left.\frac{df(a\beta(t))}{dt}\right|_{t=0}$$

$$= \left.\frac{df(\beta(t+t_0))}{dt}\right|_{t=0} = \left.\frac{df(\beta(t))}{dt}\right|_{t=t_0} = \frac{d\beta(t_0)}{dt} f,$$

i.e.

$$(dL_a)_e \frac{d\beta(0)}{dt} = \frac{d\beta(t_0)}{dt}.$$

But for $t \in I$ the curve β is an integral curve of the field X. In particular

$$\frac{d\beta(0)}{dt} = X_{\beta(0)} = X_e.$$

In addition, since X is left-invariant, we have $(dL_a)_e X_e = X_a = X_{\varphi(t_0)}$. Hence

$$X_{\varphi(t_0)} = \frac{d\beta(t_0)}{dt},$$

so that β is really an integral curve of the vector field X. □

Corollary. *Every left-invariant vector field X is complete.* □

According to Propositions 2 and 3 left-invariant fields $X \in \mathfrak{l}(G)$ and one-parameter subgroups β are in a natural bijective correspondence. If desired, therefore we may take one-parameter subgroups as the elements of a vector space $\mathfrak{l}(G)$.

Comparing the above said, we see the validity of

Theorem 1. *A space $\mathfrak{g} = \mathfrak{l}(G)$ admits the following three equivalent interpretations*:

(i) *The elements of $\mathfrak{g}$ are the left-invariant vector fields X on a Lie group G.*

(ii) *The elements of $\mathfrak{g}$ are the tangent vectors A to G at point e (the identity of G).*

(iii) *The elements of* $\mathfrak{g}$ *are the one-parameter subgroups* β *of* G.

The passage from the first interpretation to the second one is given by the correspondence

$$X \mapsto X_e,$$

the passage from the third interpretation to the second one is given by the correspondence

$$\beta \mapsto \frac{d\beta(0)}{dt}$$

and the passage from the first interpretation to the third one is given by the correspondence

$$X \mapsto \varphi_e,$$

where φ_e *is an integral curve of the field* X *passing, for* $t = 0$, *through point* e. □

The first and the second interpretation provide linear operations in $\mathfrak{g}$ relative to which $\mathfrak{g}$ is an n-dimensional vector space. How to obtain these linear operations in the third interpretation is to be discussed in Lecture 4.

Let $\Phi: G \to H$ be a homomorphism of Lie groups. Since $\Phi(e) = e$, the differential $\mathsf{T}_e\Phi = (d\Phi)_e$ of that homomorphism at the point e is a certain linear mapping of space $\mathsf{T}_e(G) = \mathfrak{l}(G)$ into space $\mathsf{T}_e(H) = \mathfrak{l}(H)$.

It is clear that correspondences $G \mapsto \mathfrak{l}(G)$ and $\Phi \mapsto (d\Phi)_e$ form a certain functor

(5) $$\mathfrak{l}: \text{GR-DIFF} \to \text{LIN}_f(\mathbb{R})$$

from the category GR-DIFF of Lie groups into the category $\text{LIN}_f(\mathbb{R})$ of finite-dimensional vector spaces over the field $\mathbb{R}$.

Definition 3. Functor (5) will be called a *Lie functor*. For the unity of notation, the mapping $(d\Phi)_e$ will also be denoted by $\mathfrak{l}(\Phi)$.

We have defined the mapping $\mathfrak{l}(\Phi)$ using the interpretation of spaces $\mathfrak{l}(G)$ as tangent spaces at point e. The question arises as to how to define the mapping $\mathfrak{l}(\Phi)$ in the other interpretations.

Recall that vector fields $X \in \mathfrak{a}(M)$ and $Y \in \mathfrak{a}(M)$ are said to be Φ-*connected*, where Φ is some smooth mapping

$M \to N$, if

(6) $\qquad Y_{\Phi a} = (d\Phi)_a\,(X_a)$ for any point $a \in M$.

In the interpretation of vector fields as linear differential operators $f \mapsto Xf$ (differentiations on M) Φ-connectedness means that for any function f (defined and smooth on some open set of the manifold N) we have $X\,(f \circ \Phi) = Yf \circ \Phi$.

If $\Phi\colon M \to N$ is a diffeomorphism, then every field $Y \in \mathfrak{a}\,(N)$ is Φ-connected with the field $\Phi^*Y \in \mathfrak{a}\,(M)$.

Proposition 4. *In the interpretation of the elements of spaces* $\mathfrak{l}\,(G)$ *as one-parameter subgroups the mapping* $\mathfrak{l}\,(\Phi)$ *is given by the formula*

$$\mathfrak{l}\,(\Phi)\,(\beta) = \Phi \circ \beta.$$

For any left-invariant vector field $X \in \mathfrak{l}\,(G)$ *and any homomorphism* $\Phi\colon G \to H$ *there is a unique left-invariant vector field* Y *on a group* H *which is* Φ*-connected with the field* X. *In the interpretation of spaces* $\mathfrak{l}\,(G)$ *as spaces of left-invariant vector fields the field* Y *is precisely the image* $\mathfrak{l}\,(\Phi)X$ *of the field* $X \in \mathfrak{l}\,(G)$ *under the mapping* $\mathfrak{l}\,(\Phi)$.

Proof. By definition

$$(d\Phi)_e\left(\frac{d\beta\,(t)}{dt}\bigg|_{t=0}\right) = \frac{d\,(\Phi \circ \beta)\,(t)}{dt}\bigg|_{t=0}.$$

Consequently, when a one-parameter subgroup β is identified with a vector $A = \dfrac{d(\beta\,(t))}{dt}\bigg|_{t=0}$ the one-parameter subgroup $\Phi \circ \beta$ is identified with the vector $(d\Phi)_eA = \mathfrak{l}\,(\Phi)A$. This proves the first statement.

The second statement follows immediately from an obvious fact that for left-invariant vector fields $X \in \mathfrak{l}\,(G)$ and $Y \in \mathfrak{l}\,(H)$ relation (6) (for $M = G$ and $N = H$) is equivalent to the equation

$$Y_e = (d\Phi_e)X_e. \quad \square$$

It is clear that tangent spaces $\mathsf{T}_e\,(G)$ and $\mathsf{T}_e\,(G_e)$ of a group G and its components of the identity G_e coincide. This means that

$$\mathfrak{l}\,(G) = \mathfrak{l}\,(G_e).$$

In the study of the Lie functor it is, therefore, possible to restrict oneself to only *connected* smooth groups G.

To illustrate the introduced notions we give an important specific example.

Recall first some general-algebraic notions which we shall constantly use.

Let $\mathbb{K}$ be an arbitrary field (in this case the field $\mathbb{R}$ of real numbers) and let $\mathcal{A}$ be a vector space over $\mathbb{K}$. Suppose that for any two elements $x, y \in \mathcal{A}$ there exists some third element $z \in \mathcal{A}$ denoted by xy and called the *product* of elements x and y. Then every element $a \in A$ will define two mappings

$$L_a: x \mapsto ax, \qquad R_a: x \mapsto xa$$

of $\mathcal{A}$ into itself.

Definition 4. A vector space $\mathcal{A}$ with a multiplication $x, y \mapsto xy$ given on it is said to be an *algebra* (over a field $\mathbb{K}$) if for every element $a \in \mathcal{A}$ the mappings $L_a : \mathcal{A} \to \mathcal{A}$ and $R_a: \mathcal{A} \to \mathcal{A}$ are linear, i.e. if

$$(7) \qquad a(x+y) = ax + ay \qquad (x+y)a = xa + ya$$

for any elements $x, y \in \mathcal{A}$ and

$$(8) \qquad k(ax) = a(kx), \qquad k(xa) = (kx)a$$

for any element $x \in \mathcal{A}$ and any element $k \in \mathbb{K}$.

Condition (7) (together with the first four vector space axioms) implies that the set $\mathcal{A}$ with the operations of addition and multiplication on it is a ring. It may be said therefore that an algebra is a ring that is at the same time a vector space in which condition (8) is satisfied, i.e. the condition

$$(9) \qquad k(xy) = (kx)y = x(ky)$$

that must hold for any elements $x, y \in \mathcal{A}$ and any element $k \in \mathbb{K}$.

A *homomorphism* of algebras is a linear mapping of one algebra into another that sends a product into a product (is a ring homomorphism).

It is clear that algebras (over a given field $\mathbb{K}$) and all their homomorphisms form a category. We shall denote that category by ALG.

A vector subspace $\mathscr{B}$ of an algebra $\mathscr{A}$ is said to be a *subalgebra* of $\mathscr{A}$ if $xy \in \mathscr{B}$ for all elements x, $y \in \mathscr{B}$. It is clear that any subalgebra is automatically an algebra.

Definition 5. An algebra in which multiplication is associative is called an *associative algebra.*

All associative algebras form a complete subcategory ALG-ASS of the category ALG. (A subcategory B of a category C is said to be a *complete subcategory* if for any objects $B_1, B_2 \in \mathsf{B}$ every morphism $B_1 \to B_2$ of C is in B.)

Every subalgebra of an associative algebra is itself associative.

Associative algebras having an identity (i.e. an element e such that $ae = ea = a$ for any element $a \in \mathscr{A}$) will be called *unital algebras.* They form a complete category ALG_0-ASS of the category ALG-ASS.

An example of a unital algebra is the *matrix algebra* $\mathbb{K}(n)$.

An element a of a unital algebra $\mathscr{A}$ is said to be *invertible* if in $\mathscr{A}$ there is an element a^{-1} such that $aa^{-1} = a^{-1}a = e$. The set $G(\mathscr{A})$ of all invertible elements of $\mathscr{A}$ is obviously a multiplicative group.

It is clear that the element a is invertible if and only if so is the linear operator L_a, i.e., when $\mathscr{A}$ is finite-dimensional, if $\det L_a \neq 0$.

For $\mathbb{K} = \mathbb{R}$ it follows that *for a finite-dimensional algebra $\mathscr{A}$ the set $G(\mathscr{A})$ is open in $\mathscr{A}$* and is, hence, a smooth manifold (of dimension $n = \dim \mathscr{A}$).

Thus $G(\mathscr{A})$ is both a group and a smooth manifold. Since multiplication in this group is bilinear, it is clearly smooth and hence (Proposition 1 of Lecture 1) *$G(\mathscr{A})$ is a Lie group.*

We find for this Lie group a vector space $\mathfrak{l}(G(\mathscr{A}))$.

To this end recall that for any finite-dimensional vector space $\mathscr{V}$ (considered as a smooth manifold) and any point $v \in \mathscr{V}$ the tangent space $\mathsf{T}_v(\mathscr{V})$ is naturally identified with $\mathscr{V}$: the identifying isomorphism

$$\mathscr{V} \to \mathsf{T}_v(\mathscr{V}) \tag{10}$$

associates with every vector $a \in \mathscr{V}$ a tangent vector at point $t = 0$ to a curve $t \mapsto v + ta$. Therefore, in particular, $\mathsf{T}_e(\mathscr{A}) = \mathscr{A}$. On the other hand, since $G(\mathscr{A})$ is open in $\mathscr{A}$, we have $\mathsf{T}_e(G(\mathscr{A})) = \mathsf{T}_e(\mathscr{A})$. Consequently, (here we use the interpretation of the vector space $\mathfrak{l}(G)$ as a tangent

space $\mathsf{T}_e(G)$):

(11) $$\mathfrak{l}(G(\mathcal{A})) = \mathcal{A}.$$

It is interesting to interpret equation (11) within the framework of the other two interpretations of the space $\mathfrak{l}(G)$.

Let $\mathscr{V}$ be a finite-dimensional vector space and let $\mathcal{A}: \mathscr{V} \to \mathscr{V}$ be a linear operator. Since A is obviously a smooth mapping of a smooth manifold $\mathscr{V}$ into itself, its differential $(dA)_v : \mathsf{T}_v(\mathscr{V}) \mapsto \mathsf{T}_{Av}(\mathscr{V})$ is defined for any point $v \in \mathscr{V}$. By definition this differential turns the tangent vector to the curve $t \mapsto v + ta$ into the tangent vector to the curve $t \mapsto A(v + ta) = Av + tAa$. This means that by virtue of identifications $\mathsf{T}_v(\mathscr{V}) = \mathscr{V}$ and $\mathsf{T}_{Av}(\mathscr{V}) = (\mathscr{V})$ the differential $(dA)_v$ coincides with the operator A. Thus *a differential of a linear operator is the linear operator itself.*

In particular, we see that $(dL_a)_e = L_a$ for any element $a \in A$.

On the other hand, by virtue of the same identifications any vector field X on $G(\mathcal{A})$ is nothing but some smooth mapping $G(\mathcal{A}) \to \mathcal{A}$. The condition of left-invariance (1) for a vector field treated in this way is, by virtue of the remark just made, of the form

(12) $$X_b = L_{a^{-1}} X_{ab}, \text{ where } a,\ b \in G(\mathcal{A})$$

from which, for $b = e$, it follows that $X_a = L_a X_e$, i.e. that the field is of the form $a \mapsto ab$, where $b = X_e \in \mathcal{A}$. Since any such field clearly satisfies condition (12), we see, on changing somewhat the notation, that all *left-invariant vector fields $G(\mathcal{A}) \to \mathcal{A}$ on a Lie group $G(\mathcal{A})$ are of the form* $x \mapsto xa$, $x \in G(\mathcal{A})$, where a is an element of $\mathcal{A}$.

Discussion of equation (11) within the framework of the third interpretation of vectors of $\mathfrak{l}(G(\mathcal{A}))$, i.e. their interpretation as one-parameter subgroups, requires some breaking of the ground.

The norm given in an algebra $\mathcal{A}$ (over a field $\mathbb{R}$) is said to be *multiplicative* if

$$\| ab \| \leqslant \| a \| \cdot \| b \|$$

for any elements a, $b \in \mathcal{A}$.

Lemma 1. *In any finite-dimensional algebra $\mathcal{A}$ over the field $\mathbb{R}$ there is a multiplicative norm.*

Proof. Given a basis $e_1, \ldots, e_n$ in $\mathcal{A}$, the formula

$$\| a \| = \max \ (| a^1 |, \ldots, | a^n |), \tag{13}$$

where $a^1, \ldots, a^n$ are the coordinates of an element a in the basis $e_1, \ldots, e_n$, will obviously define some norm in $\mathcal{A}$. We show that with an appropriate choice of the basis $e_1, \ldots, e_n$ norm (13) is multiplicative.

Suppose first that the basis $e_1, \ldots, e_n$ is arbitrary and that

$$e_i e_j = c_{ij}^k e_k, \qquad i, j, k = 1, \ldots, n.$$

Then for any elements $a = a^i e_i$ and $b = b^i e_i$ we have

$$\| ab \| = \| c_{ij}^k a^i b^j e_k \| = \max_k |c_{ij}^k a^i b^j|$$

$$\leqslant \sum_{i, j=1}^{n} \max_k |c_{ij}^k| \cdot \max_p |a^p| \cdot \max_q |b^q| = C \cdot \| a \| \cdot \| b \|,$$

where $C = n^2 \max\limits_{i, j, k} |c_{ij}^k|$. Hence for the norm

$$\| a \| = \lambda \max \ (| a^1 |, \ldots, | a^n |),$$

where $\lambda > C$ $\left(\text{this norm is norm (13) corresponding to the basis } \frac{1}{\lambda} e_1, \ldots, \frac{1}{\lambda} e_n\right)$ we have

$$\| ab \| \leqslant \frac{C}{\lambda} \| a \| \cdot \| b \| \leqslant \| a \| \cdot \| b \|,$$

i.e. this norm is multiplicative. □

Notice that in Lemma 1 the algebra $\mathcal{A}$ is *not assumed* to be associative.

This remark will be used later on, and for the time being we apply Lemma 1 to a finite-dimensional associative unit (with an identity e) algebra $\mathcal{A}$. For any element $a \in \mathcal{A}$ we consider an infinite series

$$e + ta + \frac{t^2 a^2}{2} + \ldots + \frac{t^n a^n}{n!} + \ldots . \tag{14}$$

With respect to a multiplicative norm *this series is absolutely*

convergent, i.e. the number series

$$\| e \| + \| ta \| + \left\| \frac{t^2a^2}{2} \right\| + \dots + \left\| \frac{t^n a^n}{n!} \right\| + \dots$$

is convergent (since it is majorized to the series for $e^{t\,\|a\|}$). However, the standard proof (usually given for series with numerical terms but preserved for series with vector terms as well) shows that *any absolutely convergent series converges* (in the norm and hence also coordinatewise, which in a finite-dimensional vector space is equivalent). Consequently, *series* (14) *converges.*

The sum of series (14) is denoted by e^{ta} and an $\mathcal{A}$-valued function $t \mapsto e^{ta}$ is called an *exponential function in an algebra* $\mathcal{A}$. (Of course, the letter e here has nothing to do with the identity e in the algebra $\mathcal{A}$.)

In particular, for $\mathcal{A} = \mathbb{R}(n)$ we obtain a *matrix exponential function* $t \mapsto e^{tA}$, $A \in \mathbb{R}(n)$.

For $\mathcal{A}$-valued functions $t \mapsto a(t)$ it is possible to reproduce practically all the constructions of elementary analysis. For example, the *derived function* $t \mapsto a'(t)$ is defined by the formula

(15) $$a'(t) = \lim_{\Delta t \to 0} \frac{a(t+\Delta t) - a(t)}{\Delta t}$$

and if the function $t \mapsto a(t)$ is sufficiently smooth, then

(16) $$a(t) = a(t_0) + (t - t_0)\, a'(t_0) + O(t - t_0)^2.$$

It is also possible to regard every function $t \mapsto a(t)$ as a curve in a smooth manifold $\mathcal{A}$ and hence to speak of its tangent vector $\frac{da(t)}{dt}$ at point t, which, by virtue of the general isomorphism (10), can be thought of as a vector in $\mathcal{A}$.

It turns out that these two approaches coincide, i.e.

$$a'(t) = \frac{da(t)}{dt} \text{ for any } t.$$

Indeed, by formula (15) the tangent vector to $t \mapsto a(t)$ at point $t = t_0$ coincides with the tangent vector to $t \mapsto a(t_0) + (t - t_0)\, a'(t_0)$ which by virtue of isomorphism (10) is thus identified with the vector $a'(t_0)$. □

In practice, however, definition (15) is undoubtedly more

convenient, since it yields at once all usual formulas of differentiation calculus (for instance the formula of differentiation of the product $(a(t)b(t))' = a'(t)\,b(t) + a(t)\,b'(t)$) provided all the necessary precautions resulting from a possible noncommutativity of multiplication in algebra $\mathcal{A}$ are observed (because of this, say, the formula for the derived function $t \mapsto a^{-1}(t)$ assumes the form $(a^{-1}(t))' = -a^{-1}(t)\,a'(t)\,a^{-1}(t)$).

If, however, the values of an $\mathcal{A}$-valued function $t \mapsto a(t)$ commute, i.e. $a(t)\,a(s) = a(s)\,a(t)$ for any t and s, then no reservations are necessary. Therefore, in particular, for any polynomial

$$f(X) = a_0 + a_1X + \ldots + a_mX^m$$

and any $\mathcal{A}$-valued function $a \mapsto a(t)$ with commutative values there is a formula

$$\frac{d}{dt} f(a(t)) = f'(a(t))\,a'(t), \tag{17}$$

where

$$f'(X) = a_1 + 2a_2 + \ldots + ma_mX^{m-1}.$$

This formula remains valid also when $f(X)$ is the sum of an infinite power series

$$f(X) = a_0 + a_1X + \ldots + a_nX^n + \ldots, \tag{18}$$

since in this case the necessary interchange of two passages to the limit is obviously valid (if it is assumed, of course, that $\| a(t) \|$ is in the circle of convergence of series (18)).

For series made up of $\mathcal{A}$-valued functions the usual rules for their termwise differentiation are also valid. In particular, series (14) admits a termwise differentiation. Therefore

$$\frac{de^{ta}}{dt} = a + ta^2 + \ldots + \frac{t^{n-1}a^n}{(n-1)!} + \cdots$$
$$= a\left(e + ta + \ldots + \frac{t^{n-1}a^{n-1}}{(n-1)!} + \cdots\right) = ae^{ta}.$$

Thus, *an exponential function* $t \mapsto e^{ta}$ *has the property that*

$$\frac{de^{ta}}{dt} = ae^{ta} \tag{19}$$

for any t.

It follows that the *solution of the $\mathcal{A}$-valued differential equation*

$$\frac{dx(t)}{dt} = ax(t) \tag{20}$$

subject to the initial condition

$$x(0) = c$$

is expressed by the formula

$$x(t) = e^{ta}c.$$

In fact, according to formula (17)

$$x'(t) = (e^{ta})'c = ae^{ta}c = ax(t)$$

and $x(0) = c$. On the other hand, for the vector $x(t)$ equation (20) reduces to a system of linear differential equations with constant coefficients; therefore the solution $x(t)$ exists and is unique. □

Now it is easy to see that *for any s and t*

$$e^{(t+s)a} = e^{ta}e^{sa}. \tag{21}$$

Indeed, for every fixed s the function $t \mapsto x(t) = e^{(t+s)a}$ satisfies equation (20) with the initial condition $x(0) = e^{sa}$. Therefore $x(t) = e^{ta}e^{sa}$. □

It follows from relation (21) in particular, that the *function $t \mapsto e^{ta}$ is a function with commutative values.* Hence (see formula (17)) for any power series (18) there is a formula

$$\frac{d}{dt} f(e^{ta}) = f'(e^{ta})\, ae^{ta} \tag{22}$$

(if, of course, the series for $f(e^{ta})$ is absolutely convergent).

Now let us return to the vector space $\mathfrak{l}(G)$ with $G = G(\mathcal{A})$.

One-parameter subgroups of the group $G(\mathcal{A})$ are nothing but smooth $\mathcal{A}$-valued functions $x \mapsto x(t)$ satisfying the relation

$$x(s+t) = x(s)\,x(t), \quad s, \quad t \in \mathbb{R}. \tag{23}$$

The general solution of this functional equation can now be easily found. Indeed, on differentiating (23) with respect to s and then putting $s = 0$ we obtain for $x(t)$ the already known

differential equation (20) with $a = x'(0)$. In view of the initial condition $x(0) = e$ we, therefore, get $x(t) = e^{ta}$. Since by formula (21) this solution satisfies (23), this proves that *any one-parameter subgroup of* $G(\mathcal{A})$ *is of the form* $t \mapsto e^{ta}$.

Denoting a one-parameter subgroup $t \mapsto e^{ta}$ by β_a we thus obtain a bijective correspondence $a \mapsto \beta_a$ between the elements of an algebra $\mathcal{A}$ and one-parameter subgroups of a Lie group $G(A)$. This is precisely correspondence (11) in the third interpretation.

Lecture 3

Matrix Lie groups admitting the Cayley construction • A generalization of the Cayley construction. Groups possessing ln-*images • Lie algebras. Examples of Lie algebras • Lie algebras of vector fields. The Lie algebra of a Lie group • An example: the Lie algebra of a group of invertible elements of an associative algebra • Locally isomorphic Lie groups • Local Lie groups • Lie functor on the category of local Lie groups*

The results obtained at the end of the preceding lecture also apply to the full linear group GL $(n) = G\,(\mathbb{R}\,(n))$ as well. In particular, we see that *one-parameter subgroups of* GL (n) *are the matrix exponential functions* $t \mapsto e^{tA}$ *and only these functions.*

Definition 1. A subgroup G of GL (n) is said to be a *matrix Lie group* if:

(a) a smoothness is introduced on G with respect to which it is a Lie group;

(b) the embedding $\iota : G \mapsto \mathrm{GL}\,(n)$ is smooth (and hence it is a homomorphism of Lie groups).

Every one-parameter subgroup of the group G is automatically a one-parameter subgroup of GL (n) and so is of the form $t \mapsto e^{tA}$. This defines an injective mapping $\mathfrak{l}\,(G) \to \mathfrak{l}\,(\mathrm{GL}\,(n)) = \mathbb{R}\,(n)$ which (see Proposition 5, Lecture 2) is nothing but the mapping $\mathfrak{l}\,(\iota)$. Thus, *for any matrix Lie group the vector space* $\mathfrak{g} = \mathfrak{l}\,(G)$ *is naturally identified with some subspace of the vector space* $\mathbb{R}\,(n)$.

Any group admitting the Cayley construction (see Lecture 1) is an example of a matrix Lie group, say a group $\mathrm{O}_J\,(n)$ of all J-orthogonal matrices. By definition a matrix one-parameter subgroup $t \mapsto e^{tA}$ is a one-parameter subgroup

of $O_J(n)$ if and only if for any $t \in \mathbb{R}$

$$(e^{tA})^{\mathsf{T}} J e^{tA} = J.$$

Differentiating this relation with respect to t and setting $t = 0$ we get

$$A^{\mathsf{T}} J + JA = 0.$$

This relation implies by definition that A is a J-skew-symmetric matrix. Conversely the mapping $t \to e^{tA}$ is found to be a one-parameter subgroup of $O_J(n)$ for any J-skew-symmetric matrix A.

To establish it we use the matrix analogue of the well-known elementary formula

$$e^a = \lim_{m\to\infty} \left(1 + \frac{a}{m}\right)^m.$$

We show that (with 1 replaced by e) *this formula is valid in any finite-dimensional associative algebra* $\mathcal{A}$. Indeed, since

$$\frac{1}{m^k}\binom{m}{k} = \underbrace{\frac{m(m-1)\ldots(m-k+1)}{m\cdot m\cdot\ldots\cdot m}}_{k \text{ multipliers}} \cdot \frac{1}{k!} \leqslant \frac{1}{k!}$$

for any multiplicative norm

$$\left\| e^a - \left(e + \frac{a}{m}\right)^m \right\| = \left\| \sum_{k=0}^{\infty} \left(\frac{1}{k!} - \frac{1}{m^k}\binom{m}{k}\right) a^k \right\|$$

$$\leqslant \sum_{k=0}^{\infty} \left(\frac{1}{k!} - \frac{1}{m^k}\binom{m}{k}\right) \|a\|^k$$

$$= e^{\|a\|} - \left(1 + \frac{\|a\|}{m}\right)^m,$$

and therefore

$$\lim_{m\to\infty} \left\| e^a - \left(e + \frac{a}{m}\right)^m \right\| = 0,$$

since

$$\left(1 + \frac{\|a\|}{m}\right)^m \to e^{\|a\|}. \ \square$$

We see that for any t

$$Je^{tA} = J \lim_{m\to\infty} \left(E + \frac{tA}{m}\right)^m = \lim_{m\to\infty} J \left(E + \frac{tA}{m}\right)^m$$

$$= \lim_{m\to\infty} \left(E - \frac{tA^{\mathsf{T}}}{m}\right)^m J = e^{-tA^{\mathsf{T}}} J,$$

since $Jf(A) = f(-A^{\mathsf{T}})J$ for any polynomial $f(A)$ of the matrix A. Therefore

$$(e^{tA})^{\mathsf{T}} J e^{tA} = (e^{tA})^{\mathsf{T}} e^{-tA} J = J,$$

so indeed, $e^{tA} \in \mathrm{O}_J(n)$.

This proves that *for a group* $\mathrm{O}_J(n)$ *the vector space of all J-skew-symmetric matrices is a subspace* $\mathfrak{l}(\mathrm{O}_J(n))$ *of space* $\mathbb{R}(n)$.

Comparing this statement with the result obtained in Example 7, Lecture 1, we see that the *subspace* $\mathfrak{l}(\mathrm{O}_J(n))$ *coincides with the Cayley image of* $\mathrm{O}_J(n)$. This turns out to be a general fact:

Proposition 1. *If a matrix group* $G \subset \mathrm{GL}(n)$ *admits the Cayley construction (and so is a matrix Lie group), then the corresponding vector space* $\mathfrak{l}(G)$ *coincides with the Cayley image* $G^{\#}$ of G.

Proof. Let $A \in \mathfrak{l}(G)$, i.e. let the mapping $t \mapsto e^{tA}$ be a one-parameter subgroup of the group G. Since the set G^0 of nonexceptional matrices in G is a neighbourhood of the identity E of G, there is $\varepsilon > 0$ such that for $|t| < \varepsilon$ the matrix e^{tA} is nonexceptional and therefore its Cayley image

$$(e^{tA})^{\#} = (E - e^{tA})(E + e^{tA})^{-1} \in G^{\#}$$

is defined. Since $G^{\#}$ is a vector space, it follows that the matrix

$$\left.\frac{d(e^{tA})^{\#}}{dt}\right|_{t=0} = \lim_{t\to 0} \frac{(e^{tA})^{\#}}{t}$$

also belongs to $G^{\#}$. But on the other hand

$$\frac{d(e^{tA})^{\#}}{dt} = -Ae^{tA}(E + e^{tA})^{-1} + (E - e^{tA}) \frac{d(E + e^{tA})^{-1}}{dt}$$

and therefore

$$\left.\frac{d\,(e^{tA})^{\#}}{dt}\right|_{t=0} = -\frac{1}{2}A.$$

Consequently, $A \in G^{\#}$.

This proves that $\mathfrak{l}\,(G) \subset G^{\#}$ and hence $\mathfrak{l}\,(G) = G^{\#}$ since the vector spaces $\mathfrak{l}\,(G)$ and $G^{\#}$ are of the same dimension (equal to $\dim G$). □

It follows from Proposition 1, according to the examples analyzed in Lecture 1, that the *space* $\mathfrak{l}\,(G)$ *for the orthogonal group* O (n) (*or equivalently for the group* SO (n)) *consists of skew-symmetric* $n \times n$ *matrices*; *for the real symplectic group* Sp $(m, \mathbb{R})$ *of matrices of the form*

$$\begin{pmatrix} A & B \\ C & -A^{\mathsf{T}} \end{pmatrix},$$

where B *and* C *are symmetric* $m \times m$ *matrices and* A *is an arbitrary matrix*;

for the orthogonal symplectic group Sp $(m) \cap$ O $(2m)$ *of matrices of the form*

$$\begin{pmatrix} A & -C \\ C & A \end{pmatrix},$$

where A *is a skew-symmetric matrix and* C *a symmetric matrix*;

for the unitary group U (n) *of skew-Hermitian matrices*;

for the group Up (m) *of matrices of the form*

$$\begin{pmatrix} A & B \\ C & -\overline{A}^{\mathsf{T}} \end{pmatrix},$$

where B *and* C *are Hermitian* $m \times m$ *matrices and* A *is an arbitrary matrix*;

for the symplectic group Sp (m) *of matrices of the form*

$$\begin{pmatrix} A & B \\ -\overline{B} & \overline{A} \end{pmatrix},$$

where A *is a skew-Hermitian matrix and* B *is a symmetric* $m \times m$ *matrix.* □

The statement that a group admitting the Cayley construction is a matrix Lie group is not strictly related to the

Cayley mapping $A \mapsto A^{\#}$ and can be substantially generalized.

As above, it will be convenient to identify $\mathbb{R}^{n^2}$ with the space $\mathbb{R}(n)$ of all square $n \times n$ matrices.

Proposition 2. *A subgroup G of the group* GL (n) *is a matrix Lie group if there is a diffeomorphism $f\colon V \to \mathring{V}$ of some neighbourhood V of the identity matrix in* GL (n) *onto an open set $\mathring{V}$ of $\mathbb{R}(n)$ that has the property that the set $f(G \cap V)$ is the intersection of $\mathring{V}$ and some vector subspace $G^{\#}$ of the space $\mathbb{R}(n)$:*

$$f(G \cap V) = G^{\#} \cap \mathring{V}.$$

Proof. Let $m = \dim G^{\#}$ and let $\varphi\colon G^{\#} \to \mathbb{R}^m$ be an isomorphism of the space $G^{\#}$ onto the space $\mathbb{R}^m$. Also let $U = G \cap V$ and $\mathring{U} = \varphi(G^{\#} \cap \mathring{V})$. Then $\mathring{U}$ is an open set in $\mathbb{R}^m$ and the mapping $h = \varphi \circ f$ onto U is a bijective mapping $U \to \mathring{U}$. In other words, the pair (U, h) is a chart on G.

Now let A be an arbitrary matrix in G and let $U_A = L_A(U)$ and $h_A = h \circ L_A^{-1}$. Then the pair (U_A, h_A) is also a chart on G. Since $A \in U_A$, all sets of the form U_A cover G. Furthermore, if $U_A \cap U_B \neq \varnothing$, then on $h_A(U_A \cap U_B)$ the mapping $h_B \circ h_A^{-1}$ will be a restriction of the diffeomorphism

$$h \circ L_B^{-1} \circ L_A \circ h^{-1} = \varphi \circ f \circ L_{B^{-1}A} \circ f^{-1} \circ \varphi^{-1}$$

and hence it will itself be a diffeomorphism. Consequently, charts (U_A, h_A) make up an atlas. This defines on G a smoothness with respect to which G is obviously a matrix Lie group. $\square$

A case of a group admitting the Cayley construction arises when V is the set of all nonexceptional matrices in G and $f\colon V \to \mathring{V}$ is a Cayley mapping (and consequently the vector space $G^{\#}$ is the Cayley image of G).

Proposition 1 is also carried over to the general case being considered if we require that $f\colon V \to \mathring{V}$ be an *analytic* diffeomorphism, i.e. that the following conditions be satisfied:

(a) there is a number R and a matrix norm $\| \ \|$ such that $\| A - E \| < R$ for any matrix $A \in V$;

(b) there exists a series

$$f(z) = a_0 + a_1(z-1) + \ldots + a_m(z-1)^m + \ldots$$

convergent for $|z-1| < R$ such that for any matrix $A \in V$

$$f(A) = a_0E + a_1(A-E) + \ldots + a_m(A-E)^m + \ldots$$

(in view of condition (a) this equation makes sense);

(c) the number $a_1 = f'(1)$ is other than zero.

Proposition 3. *If for a subgroup G of a group* GL (n) *there is an analytic diffeomorphism $f\colon V \to \mathring{V}$ which satisfies the conditions of Proposition 2, then the vector space $\mathfrak{l}(G)$ corresponding to that group coincides with the vector space $G^\#$ specified in Proposition 2.*

Proof. (cf. the proof of Proposition 1). Let $t \mapsto e^{tA}$ be an arbitrary one-parameter subgroup of a group G and let $\varepsilon > 0$ be a number such that for $|t| < \varepsilon$ the matrix e^{tA} belongs to V. Then $e^{tA} \in G \cap V$ and hence $f(e^{tA}) \in G^\# \cap \mathring{V}$. Therefore $\frac{df(e^{tA})}{dt} \in G^\#$ and, in particular,

$$\left.\frac{df(e^{tA})}{dt}\right|_{t=0} \in G^\#.$$

But according to formula (22) of Lecture 2

$$\left.\frac{df(e^{tA})}{dt}\right|_{t=0} = f'(e^{tA})\,Ae^{tA}\Big|_{t=0} = a_1A,$$

since

$$f'(z) = a_1 + 2a_2(z-1) + \ldots + ma_m(z-1)^{m-1} + \ldots$$

and hence $f'(E) = a_1E$. Consequently, $a_1A \in G^\#$ and therefore $A \in G^\#$, for under the hypothesis $a_1 \neq 0$.

This proves that $\mathfrak{l}(G) \subset G^\#$. Therefore $\mathfrak{l}(G) = G^\#$, since these vector spaces are of the same dimension. □

To construct the diffeomorphism f in explicit form, we consider the matrix series

$$\ln A = (A-E) - \frac{1}{2}(A-E)^2 + \ldots + \frac{(-1)^{m+1}}{m}(A-E)^m + \ldots,$$

which converges when $\|A-E\| < 1$ (where $\|\ \|$ is a matrix

multiplicative norm, say the norm $\| A \| = n \cdot \max\limits_{i,j} a_{ij})$. A trivial calculation repeating the familiar calculation for number series shows that $e^{\ln A} = A$ when $\| A - E \| < 1$ (i.e. when the matrix $\ln A$ is defined).

It is interesting that on the contrary the equation $\ln e^A = A$ may fail to hold even when the matrix $\ln e^A$ is defined (in the sense that for the matrix $B = e^A$ the series $\ln B$ converges). Indeed, if

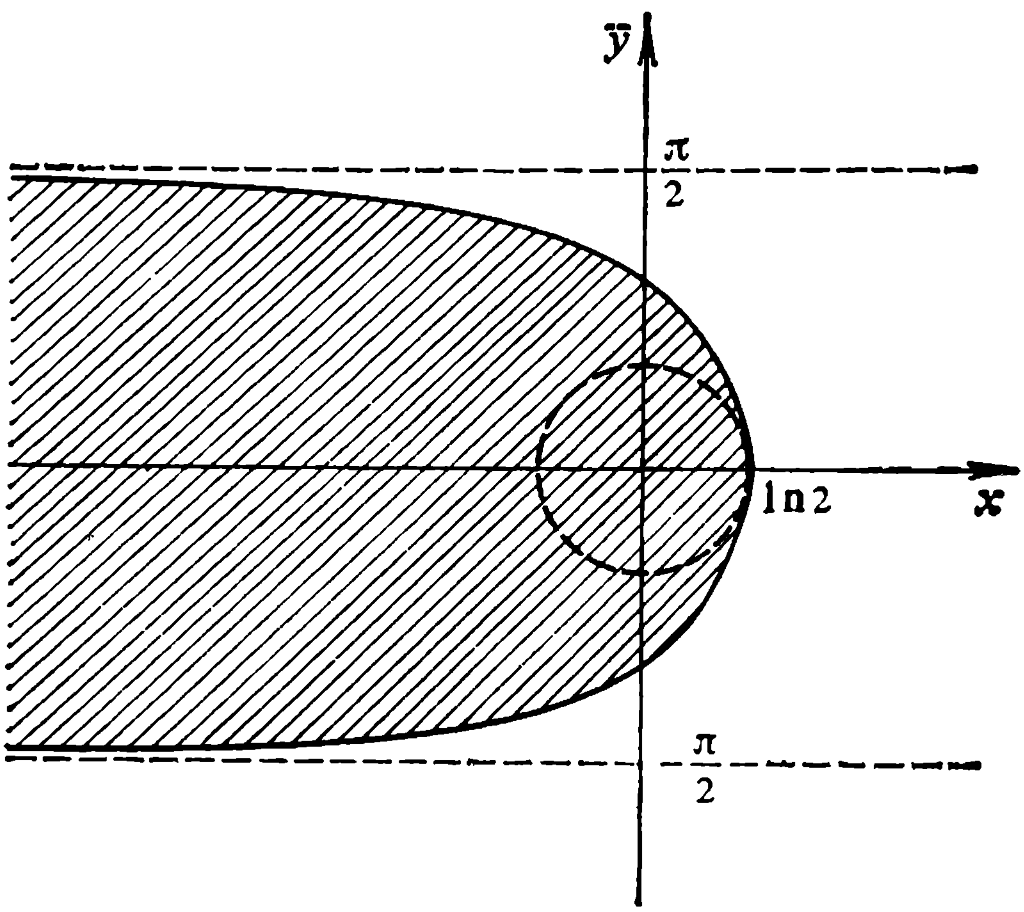
$$A = \begin{pmatrix} 0 & -\theta \\ \theta & 0 \end{pmatrix},$$

then a straightforward calculation shows that

$$e^A = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

and therefore for $\theta = 2\pi$ we get $e^A = E$. Consequently the matrix $\ln e^A$ is defined and equals zero, not A.

A similar statement is also valid for complex numbers. For example, if $e^{2\pi i} = 1$, then $\ln e^{2\pi i} = 0$. The proof is



clear. The condition $| e^z - 1 | < 1$ defines in the plane of the complex variable $z = x + iy$ a countable system of regions resulting from one another by $2\pi i$ shifting, and

within $|y| < \frac{\pi}{2}$, the corresponding region is bounded by the curve $e^x = 2\cos y$ (see the figure). On the other hand, a formal transformation of the series $\ln e^z$ into the series z is meaningful, like any transformation of series, only in the corresponding circle of convergence, which in the given case is the maximal circle with centre at $z_0 = 0$ and contained in the region under consideration. Since the radius of that circle is equal to $\ln 2$, we can be sure that $\ln e^z = z$ only if $|z| < \ln 2$.

It is now clear that the same formal transformations will do for the series $\ln e^A$ as well and consequently the *equation* $\ln e^A = A$ *obviously holds for* $\|A\| < \ln 2$.

This proves that the mapping $\ln: A \to \ln A$ realizes a diffeomorphism of some neighbourhood $\mathring{V}$ of the identity matrix in the group GL (n) onto a certain neighbourhood $\mathring{V}$ of the zero matrix in the vector space $\mathbb{R}(n)$ (with the inverse diffeomorphism $\exp: A \mapsto e^A$).

We shall say that a *subgroup* $G \in \mathrm{GL}(n)$ *possesses an* ln-*image* if there is a vector subspace $G^\flat$ in $\mathbb{R}(n)$ such that

$$\ln(G \cap V) = G^\flat \cap \mathring{V}.$$

By Proposition 2 such a subgroup is a matrix Lie group and by Proposition 3 the vector space $G^\flat$ coincides with the vector space $\mathfrak{g} = \mathfrak{l}(G)$.

Unlike the Cayley construction, this construction allows us to prove at once that the *groups* SL (n) *and* SU (n) *of unimodular matrices are matrix Lie groups.* Indeed, it is known that $\det e^A = e^{\mathrm{Tr}\,A}$, where $\mathrm{Tr}\,A$ is the *trace* of the matrix A (the sum of its diagonal elements). Therefore the condition that the matrix e^A be unimodular is equivalent to the linear condition $\mathrm{Tr}\,A = 0$ on the matrix A. □

(It is easy to see that it suffices to prove the equation $\det e^A = e^{\mathrm{Tr}\,A}$ only for matrices having a Jordan or at least triangular form. But for such a matrix A the matrix e^A is also triangular, and its diagonal elements are of the form $e^{a_1}, \ldots, e^{a_n}$, where $a_1, \ldots, a_n$ are diagonal elements of the matrix A. Therefore $\det e^A = e^{a_1} \ldots e^{a_n} = e^{a_1 + \ldots a_n} e^{\mathrm{Tr}\,A}$.)

But the main advantage of the ln-construction over the Cayley construction is that it is universal.

Proposition 4. *Every matrix Lie group G possesses an* ln-*image.*

Proof. According to the foregoing the only candidate for the role of the vector space $G^\flat$ is the vector space $\mathfrak{l}(G)$. We show that it indeed has the necessary property.

Suppose as before that V and $\mathring{V}$ are neighbourhoods (of the identity and zero matrices, respectively) such that the function $A \mapsto \ln A$ defines a diffeomorphism $\ln\colon V \to \mathring{V}$ with the inverse diffeomorphism $\exp\colon \mathring{V} \to V$. Then for any matrix $A \in \mathfrak{l}(G) \cap \mathring{V}$ there is an inclusion $e^A \in G \cap V$ (as $e^{tA} \in G$ for any t). Since $\ln e^A = A$, this proves that $\mathfrak{l}(G) \cap \mathring{V} \subset \ln(G \cap V)$.

Conversely, let $B \in G \cap V$. Then a matrix $A = \ln B \in \mathring{V}$ is defined. Consider on $\mathrm{GL}(n)$ the corresponding left-invariant vector field $Y\colon P \mapsto PA$. The restriction $X = Y|_G$ of the field Y to G is obviously a smooth left-invariant vector field on G (an element of the vector space $\mathfrak{l}(G)$) which is ι-connected with the field Y, where $\iota\colon G \to \mathrm{GL}(n)$ is an embedding. According to Proposition 4, Lecture 2, this means that $\mathfrak{l}(\iota) X = Y$. Consequently, by virtue of our general identifications the field X is identified with the matrix A. Hence $A \in \mathfrak{l}(G)$. This proves that $\ln(G \cap V) \subset \mathfrak{l}(G) \cap \mathring{V}$.

Thus $\ln(G \cap V) = \mathfrak{l}(G) \cap \mathring{V}$, which proves Proposition 4. □

So *a matrix group is a Lie group if and only if it possesses an* ln-*image*. The passage to an ln-image may be said to linearize the group, which substantially simplifies its study. Since the space $\mathfrak{l}(G)$ (coinciding for matrix groups with the ln-image) is defined for any Lie groups, it is natural to expect that the Lie functor $\mathfrak{l}\colon G \mapsto \mathfrak{l}(G)$ plays in the theory of arbitrary Lie groups a role similar to that of the functor ln in the theory of matrix Lie groups. It turns out to be really the case, and this fact is the basis of the entire Lie group theory. It is on the whole to the discussion of all these questions that our course will be devoted.

Definition 2. An algebra $\mathfrak{g}$ is said to be a *Lie algebra*, if multiplication is anticommutative in it, i.e.

$$xy = -yx$$

for any elements $x, y \in \mathfrak{g}$ and in addition for any elements $x, y, z \in y$ we have

$$(xy)z + (yz)x + (zx)y = 0, \tag{1}$$

the so-called *Jacobi identity.*

It is customary to denote Lie algebras by small Gothic letters.

For any element a of a Lie algebra $\mathfrak{g}$ the mappings L_a and R_a differ only in sign ($L_a = -R_a$). For Lie algebras it is customary to denote the mapping L_a by ad a.

Just as associative algebras, all Lie algebras form a complete subcategory of the category ALG.

We shall denote this subcategory by ALG-LIE.

Of particular importance to us will be finite-dimensional Lie algebras over the field $\mathbb{R}$. They form a category we shall denote by ALG_f-LIE.

Notice that every subalgebra of a Lie algebra is itself a Lie algebra.

A wealth of examples of Lie algebras can be obtained using the following general construction.

Let $\mathcal{A}$ be an associative algebra.

For any two elements $x, y, \in \mathcal{A}$ we define their *commutator* $[x, y]$ (also called their *Lie bracket*) by the formula

$$[x, y] = xy - yx.$$

It is clear that $[x, y] = -[y, x]$. In addition

$$\begin{aligned}[][x, y], z] + [[y, z] x] + [[z, x], y]\\ = (xy - yx)z - z(xy - yx) + (yz - zy)x - x(yz-zy)\\ + (zx - xz)y - y(zx - xz) = 0\end{aligned}$$

for any $x, y, z \in \mathcal{A}$. This means that relative to the operation $x, y \mapsto [x, y]$ (which is obviously linear in both arguments) the vector space $\mathcal{A}$ is a Lie algebra. That algebra will be called a *commutator Lie algebra* of the associative algebra $\mathcal{A}$ and denoted by $[\mathcal{A}]$.

Since any homomorphism of associative algebras is obviously a homomorphism of the corresponding commutator

algebras, the correspondence $\mathcal{A} \mapsto [\mathcal{A}]$ is some functor from the category ALG-ASS into the category ALG-LIE.

It is also often convenient to denote by $[x, y]$ a product in an arbitrary Lie algebra (which is not generally speaking a commutator Lie algebra of any associative algebra).

In this notation, the mapping ad a: $\mathfrak{g} \to \mathfrak{g}$ for any Lie algebra $\mathfrak{g}$ will be defined by the formula

$$(\text{ad } a)\, x = [a, x], \qquad a, x \in \mathfrak{g}.$$

An example of a commutator Lie algebra is the commutator Lie algebra $[\text{End}\, \mathcal{V}]$ of the associative algebra $\text{End}\, \mathcal{V}$ of all endomorphisms (linear operators) of a vector space $\mathcal{V}$. When $\mathcal{V}$ is an algebra itself (not necessarily associative), the algebra $[\text{End}\, \mathcal{V}]$ has the vector subspace $D(\mathcal{V})$ of all *differentiations* of the algebra $\mathcal{V}$ i.e. of linear mappings $D: \mathcal{V} \to \mathcal{V}$ such that

$$D(xy) = Dx \cdot y + x \cdot Dy$$

for any elements $x, y \in \mathcal{V}$. A straightforward calculation shows that for any $D_1, D_2 \in \mathcal{D}(\mathcal{V})$ the commutator $[D_1, D_2] = D_1D_2 - D_2D_1$ belongs to $\mathcal{D}(\mathcal{V})$, i.e. that the vector space $\mathcal{D}(\mathcal{V})$ is a subalgebra of the Lie algebra $[\text{End}\, \mathcal{V})$. *For any algebra $\mathcal{V}$ the vector space $\mathcal{D}(\mathcal{V})$ is thus a Lie algebra relative to the operation $D_1, D_2 \mapsto D_1D_2 - D_2D_1$.*

Suppose now that $\mathfrak{g}$ is an arbitrary Lie algebra (in which multiplication is denoted by $[x, y]$).

The Jacobi identity (1) can be rewritten using anticommutativity in any of the following two forms:

$$[a, [x, y]] = [[a, x,], y] + [x [a, y]], \quad a, x, y \in \mathfrak{g},$$

$$[[a, b], x] = [a, [b, x]] - [b, [a, x]], \quad a, b, x \in \mathfrak{g}.$$

The first of the identities is equivalent to the statement that *for any element $a \in \mathfrak{g}$ the mapping*

$$(\text{ad } a)\, x = [a, x], \qquad x \in \mathfrak{g},$$

is a differentiation of a Lie algebra $\mathfrak{g}$ and the second to the statement that the *resulting mapping $a \mapsto$* ad a *of* $\mathfrak{g}$ *into* $\mathcal{D}(\mathfrak{g})$ *is a homomorphism.*

Differentiations of the form ad a are called *interior differentiations* of the Lie algebra $\mathfrak{g}$. We thus see that the *collection*

ad $\mathfrak{g}$ *of all interior differentiations of a Lie algebra* $\mathfrak{g}$ *is a Lie algebra which is a homomorphic image of the algebra* $\mathfrak{g}$.

In the theory of smooth manifolds Lie algebras (over the field $\mathbb{R}$) arise as algebras of vector fields.

Let M be a smooth manifold and let $\mathfrak{a}(M)$ be a vector space of vector fields over M. Recall that every field $X \in \mathfrak{a}(M)$ may be considered as a differentiation on M (a linear differential operator), i.e. as some rule associating with every open set $U \subset M$ a differentiation X_U on the algebra $\mathscr{F}(U)$ of smooth functions on U and having the property that for any open set $V \subset U$ and any function $f \in \mathscr{F}(U)$ we have $X_V(f|_V) = (X_U f)|_V$. Therefore for any two fields $X, Y \in \mathfrak{a}(M)$ and any open set $U \subset M$ a differentiation $[X_U, Y_U]$ of the algebra $\mathscr{F}(U)$ is defined. Since, as can be easily seen, for every open set $V \subset U$ and any function $f \in \mathscr{F}(U)$

$$[X_V, Y_V)(f|_V) = ([X_U, Y_U] f)|_V,$$

differentiations $[X_U, Y_U]$ make up some vector field.

Definition 3. A vector field on M, which associates the differentiation $[X_U, Y_U]$ of the algebra $\mathscr{F}(U)$ with every open set $U \subset M$, is called the *Lie bracket* of fields X, Y and denoted by $[X, Y]$. Thus by definition

$$[X, Y]_U = [X_U, Y_U].$$

It is obvious that a vector space $\mathfrak{a}(M)$ is a Lie algebra relative to the operation $X, Y \mapsto [XY]$. That algebra is called the *Lie algebra of vector fields* on a manifold M. In general that algebra is infinite-dimensional.

A straightforward calculation shows that in *every chart* $(U, x^1, \ldots, x^n)$ *the components* $[X, Y]^i$, $i = 1, \ldots, n$, *of the field* $[X, Y]$ *are expressed in terms of the components* X^i *and* Y^i, $i = 1, \ldots, n$, *of the fields* X *and* Y *by the formula*

$$(2) \qquad [X, Y]^i = X^j \frac{\partial Y^i}{\partial x^j} - Y^j \frac{\partial X^i}{\partial x^j}, \quad i, j = 1, \ldots, n.$$

Indeed

$$[X, Y]^i = [X, Y]x^i = X(Yx^i) - Y(Xx^i)$$
$$= X(Y^i) - Y(X^i) = X^j \frac{\partial Y^i}{\partial x^j} - Y^j \frac{\partial X^i}{\partial x^j}. \ \square$$

It is as easy to show that *if for some smooth mapping* $\Phi\colon M \to N$ *the fields* X *and* Y *on the manifold* M *are* Φ*-connected respectively with the fields* X' *and* Y' *on the manifold* N, *then the field* $[X, Y]$ *is also* Φ*-connected with the field* $[X', Y']$. Indeed, the Φ-connectedness of X, Y and X', Y' implies that for any function f (defined and smooth in some open subset of the manifold N)

$$X(f \circ \Phi) = X'f \circ \Phi \text{ and } Y(f \circ \Phi) = Y'f \circ \Phi.$$

But then

$$\begin{aligned}[X, Y](f \circ \Phi) &= X(Y(f \circ \Phi)) - Y(X(f \circ \Phi))\\ &= X(Y'f \circ \Phi) - Y(X'f \circ \Phi)\\ &= X'(Y'f) \circ \Phi - Y'(X'f) \circ \Phi\\ &= [X', Y') f \circ \Phi\end{aligned}$$

and hence the fields $]X, Y]$ $[X', Y']$ are also Φ-connected. □

In particular, we see that for *any diffeomorphism* $\Phi\colon M \to N$

$$\Phi^*[X, Y] = [\Phi^*X, \Phi^*Y],$$

where X and Y are arbitrary vector fields on N.

For left-invariant vector fields *on a Lie group* G it immediately follows that the *Lie bracket* $[X, Y]$ *of two left-invariant vector fields* X *and* Y *is also a left-invariant vector field.* This means that a vector space $\mathfrak{g} = \mathfrak{l}(G)$ of left-invariant vector fields is a subalgebra of the Lie algebra $\mathfrak{a}(G)$ of all fields and is therefore a Lie algebra itself.

Definition 4. A Lie algebra $\mathfrak{g} = \mathfrak{l}(G)$ over the field $\mathbb{R}$ is called a *Lie algebra of a Lie group* G.

Note that we have constructed the Lie bracket $[X, Y]$ on the vector space $\mathfrak{l}(G)$ using the first interpretation of this space. No straightforward construction of this bracket within the framework of the second interpretation ($\mathfrak{l}(G) = \mathsf{T}_e(G)$) exists. How to construct the Lie bracket using the third interpretation (i.e. with elements of the space $\mathfrak{l}(G)$ interpreted as one-parameter subgroups) will be shown later.

As we know, any homomorphism $\Phi\colon G \to H$ of Lie groups induces some linear mapping $\mathfrak{l}(\Phi)\colon \mathfrak{l}(G) \to \mathfrak{l}(H)$, with the field $\mathfrak{l}(\Phi)X \in \mathfrak{l}(H)$ being Φ-connected, for any

field $X \in \mathfrak{l}(G)$, with the field X. This mapping therefore is a homomorphism of Lie algebras.

Thus the Lie functor $\mathfrak{l}: \text{GR-DIFF} \to \text{LIN}_f(\mathbb{R})$ is in fact a functor

$$\mathfrak{l}: \text{GR-DIFF} \to \text{ALG}_f\text{-LIE}$$

from the category of Lie groups into the category ALG_f-LIE of finite-dimensional Lie algebras over the field $\mathbb{R}$ (more precisely the functor $\text{GR-DIFF} \to \text{LIN}_f(\mathbb{R})$ is a composition of the functor $\text{GR-DIFF} \to \text{ALG}_f\text{-LIE}$ and the forgetful functor $\text{ALG}_f\text{-LIE} \to \text{LIN}_f(\mathbb{R})$.).

We calculate the Lie bracket for matrix Lie groups. Since for any matrix Lie group G the algebra $\mathfrak{l}(G)$ is obviously a subalgebra of the algebra $\mathfrak{l}(\text{GL}(n) = \mathfrak{gl}(n)$, it suffices to calculate the bracket only in the algebra $\mathfrak{gl}(n)$.

We perform calculation at once for a group of the form $G(\mathcal{A})$, where $\mathcal{A}$ is a finite-dimensional associative algebra.

As was established in Lecture 2, the vector space $\mathfrak{l}(G)$ for the group $G = G(\mathcal{A})$ is naturally identified with the vector space $\mathcal{A}$. Moreover, in this identification the left-invariant vector field on $G(\mathcal{A})$ corresponds to the element $x \in \mathcal{A}$, the field being in the form $x \mapsto xa$, $x \in G(\mathcal{A})$, which is considered as a mapping $G(\mathcal{A}) \mapsto \mathcal{A}$.

Let $e_1, \ldots, e_n$ be a basis of an algebra $\mathcal{A}$ and let just as in Lecture 2

$$e_ie_j = c_{ij}^k e_k, \qquad i, j, k = 1, \ldots, n,$$

where $c_{ij}^k \in \mathbb{R}$. The coordinates $x^1, \ldots, x^n$ of the elements of the algebra $\mathcal{A}$ relative to the basis $e_1, \ldots, e_n$ are local coordinates at any point $x \in G(\mathcal{A})$, with the basis $\left(\frac{\partial}{\partial x^1}\right)_x, \ldots,$

$\left(\frac{\partial}{\partial x^n}\right)_x$ of the tangent space $\mathsf{T}_x(G(\mathcal{A}))$ corresponding to

the basis $e_1, \ldots, e_n$ under identification $\mathsf{T}_x(G(\mathcal{A})) = \mathcal{A}$. Hence, with vector fields on $G(\mathcal{A})$ identified with the mappings $G(\mathcal{A}) \to \mathcal{A}$, the vector field $X = X^i \frac{\partial}{\partial x^i}$ has the corresponding mapping $x \mapsto X^i e_i$.

Since $xa = c_{jk}^i x^j a^k e_i$ for $x = x^j e_j$, $a = a^k e_k$, it follows

that in the basis $\frac{\partial}{\partial x^1}, \ldots, \frac{\partial}{\partial x^n}$ the left-invariant vector field $X: x \mapsto xa$ corresponding to the element $a \in \mathcal{A}$ has the coordinates

$$X^i = c^i_{jk} x^j a^k.$$

For any left-invariant vector fields X and Y on $G(\mathcal{A})$, therefore, the coordinates $[X, Y]^l$ of their Lie bracket will be expressed by the formula

$$\begin{aligned}[X, Y]^l &= X^k \frac{\partial Y^l}{\partial x^k} - Y^k \frac{\partial X^l}{\partial x^k} \\ &= c^k_{ij} x^i a^j \cdot c^l_{km} b^m - c^k_{ij} x^i b^j \cdot c^l_{km} a^m \\ &= c^l_{km} (c^k_{ij} x^i a^j)\, b^m - c^l_{km} (c^k_{ij} x^i b^j)\, a^m,\end{aligned}$$

where a and b are the elements of $\mathcal{A}$ corresponding to the fields X and Y. But this formula implies that the numbers $[X, Y]^l$ are the coordinates of a point $xa \cdot b - xb \cdot a = x(ab - ba)$ and that hence the field $[X, Y]$ has the corresponding element $ab - ba = [a, b]$. This proves that by virtue of identification $\mathfrak{l}(G(\mathcal{A})) = \mathcal{A}$ the *commutator Lie algebra* $[\mathcal{A}]$ *of the associative algebra* $\mathcal{A}$ *is a Lie algebra of a Lie group* $G(\mathcal{A})$.

In particular, a *Lie algebra* $\mathfrak{gl}(n)$ *of the Lie group* $\mathrm{GL}(n)$ *is the commutator algebra* $[\mathbb{R}(n)]$ *of the matrix algebra* $\mathbb{R}(n)$.

But for an arbitrary matrix group G the Lie algebra $\mathfrak{l}(G)$ is the corresponding subalgebra of the Lie algebra $[\mathbb{R}(n)] = \mathfrak{gl}(n)$.

Our further aim is to study in detail the Lie functor $\mathfrak{l}$ and, in particular, to find out to what extent and how this functor can be inverted, i.e. to what extent a Lie group G can be reconstructed from its Lie algebra $\mathfrak{g} = \mathfrak{l}(G)$.

It has already been noticed in the preceding lecture that $\mathfrak{l}(G) = \mathfrak{l}(G_e)$, where G_e is a component of the identity of a group G. In stricter terms that equation states that the homomorphism of embedding $G_e \to G$ induces an isomorphism $\mathfrak{l}(G_e) \approx \mathfrak{l}(G)$ of vector spaces. But since a homomorphism of Lie groups induces a homomorphism of Lie algebras the isomorphism $\mathfrak{l}(G_e) \approx \mathfrak{l}(G)$ is an isomorphism of Lie algebras as well. In other words, the *equation* $\mathfrak{l}(G_e) = \mathfrak{l}(G)$ *holds for Lie algebras.*

It is expedient therefore to pose the question of invertibility of the functor $\mathfrak{l}$: GR-DIFF $\to$ ALG$_f$-LIE only for *connected* Lie groups.

A complete subcategory of GR-DIFF generated by connected Lie groups will be denoted by GR$_0$-DIFF. The restriction of the Lie functor to that subcategory will also be called a *Lie functor*. According to the foregoing there is a commutative diagram of functors

$$\begin{tikzcd}
\text{GR-DIFF} \arrow[d] \arrow[dr] & \\
& \text{ALG}_f\text{-LIE} \\
\text{GR}_0\text{-DIFF} \arrow[ur] &
\end{tikzcd}$$

where the right-inclined arrows are Lie functors and the left vertical arrow is the functor of the "component of the identity" which associates the identity component with every Lie group. That diagram is a formal representation of the equation $\mathfrak{l}(G_e) = \mathfrak{l}(G)$ in functor terms.

Will a Lie functor be invertible on the category GR$_0$-DIFF i.e. more precisely, will groups with isomorphic Lie algebras be isomorphic? The answer turns out to be no.

Consider, for example, an additive group $\mathbb{R}$ of real numbers and a multiplicative group $\mathbb{S}^1$ of complex numbers equal to unity in absolute value. Both groups have a one-dimensional Lie algebra. But by virtue of anticommutativity multiplication in any one-dimensional Lie algebra (over the field $\mathbb{R}$) is trivial (the product of any two elements is zero). Hence Lie algebras of the groups $\mathbb{R}$ and $\mathbb{S}^1$ are isomorphic, whereas the groups themselves are not (one of them is compact and the other is not).

The reason why Lie algebras in that example coincide is clear: the groups $\mathbb{R}$ and $\mathbb{S}^1$ are locally (in the neighbourhood of the identity) "constructed identically".

This suggests that the relation of "local isomorphism" should be introduced for connected Lie groups, assuming groups G and H to be *locally isomorphic* if some neighbourhood U of the identity of G can be diffeomorphically mapped onto some neighbourhood V of the identity of H so that the product xy of any two elements x and y from U should turn

into the product $\overline{xy}$ of the corresponding elements $\bar{x}$, and $\bar{y}$ if xy belongs to U. It is obvious that *Lie algebras of two locally isomorphic Lie groups are isomorphic* and it may be hoped (at least the above example does not contradict this) that conversely *Lie groups with isomorphic Lie algebras are locally isomorphic*. It turns out that this is indeed the case. A major aim of this book will be to prove this basic fact. We proceed to prove this in the next lecture but the proof will be finally concluded only in Lecture 9.

However, the notion of local isomorphism of "global" Lie groups does not seem very convenient from a general methodological stand. Experience in constructing mathematical theories suggests that such a mixture of global and local aspects should lead to awkward formulations and unjustified complications of proofs. We must always try from the outset to separate clearly local from global questions.

For a particular case of Lie groups these general considerations justify introducing a new mathematical concept of a local Lie group which is a formalization of a neighbourhood of the identity in a Lie group together with the multiplication available in that neighbourhood.

Definition 5. A smooth manifold G is said to be a *local Lie group* if:

(i) some element e called the *identity element* (or *identity*) is singled out in it;

(ii) the neighbourhood $U \subset G \times G$ of the element (e, e) and the neighbourhood $U_0 \subset G$ of e are singled out;

(iii) a smooth mapping

$$U \to G \tag{3}$$

called *multiplication* and a smooth mapping

$$U_0 \to G \tag{4}$$

called the operation of taking the *inverse element* are given; the image of a point $(x, y) \in U$ under mapping (3) is denoted by xy and the image of a point $x \in U_0$ under mapping (4) by x^{-1}.;

(iv) $e^{-1} = e$,

(v) if $(x, e) \in U$, then $xe = x$; if $(e, x) \in U$, then $ex = x$;

(vi) if $(x, y) \in U$, $(y, z) \in U$, $(xy, z) \in U$ and $(x, yz) \in U$, then

$$(xy)\,z = x\,(yz);$$

(vii) if $(x, y) \in U$, $y \in U_0$ and $(xy, y^{-1}) \in U$, then

$$(xy)y^{-1} = x,$$

and similarly if $(x, y) \in U$, $x \in U_0$ and $(x^{-1}, xy) \in U$, then

$$x^{-1}\,(xy) = y.$$

In short, G is a local Lie group if for two elements x and y close enough to the identity e the product xy and an inverse element x^{-1} smoothly dependent on x, y are defined, with all group axioms holding each time whenever the objects participating in those axioms are defined.

A guideline example of a local Lie group is an arbitrary neighbourhood of the identity in an arbitrary Lie group.

In spite of the fact that Definition 5 is apparently natural it is really unsatisfactory, for it does not reflect all the aspects of the intuitive notion we mean to formalize. Indeed, it is natural to assume that the two distinct neighbourhoods of identity in a given Lie group lead to the same local Lie group, whereas by Definition 5 these local groups will be distinct.

To put the matter straight, we notice that any open set H of a local Lie group G that contains the identity e is straightforwardly a local Lie group. Every such a local group is called a *part* of the local group G. Two local Lie groups are said to be *equivalent* if some of their parts coincide. The class of equivalent local Lie groups is called a *germ* of local Lie groups (cf. the definition of germs of smooth functions in the theory of smooth manifolds.)

Germs of local Lie groups are precisely an adequate formalization of the intuitive notion of a Lie group considered locally. A consistent use of germs, however, makes the presentation cumbersome. In practice a simpler manner of presentation (that we shall also follow) has been developed when, while speaking of local Lie groups, we in fact tacitly imply their germs. The passages to equivalent local groups required in the course of the discussion are either not mentioned at all or referred to only in some most "acute" cases.

It is strongly recommended that the reader should himself convert all further discussions to a stricter presentation, clearly distinguishing local Lie groups and their germs.

Definition 6. A *homomorphism* of a local Lie group G into a local Lie group H is a smooth mapping Φ of some neighbourhood V of the identity of G into H such that

$$\Phi(xy) = \Phi x \cdot \Phi y$$

whenever the elements $\Phi(xy)$ and $\Phi x \cdot \Phi y$ are defined. If G_1 and H_1 are parts of G and H and if $\Phi(V \cap G_1) \subset H_1$, then Φ defines some homomorphism of the local Lie group G_1 into the local Lie group H_1, which is called a *part* of the homomorphism Φ. Two homomorphisms are said to be *equivalent* if they have a part in common. The class of equivalent homomorphisms is called a *germ of homomorphisms* (or a *homomorphism of the germs*).

All the local Lie groups and their homomorphisms (more precisely the germs of local Lie groups and their homomorphisms) naturally form a certain category which will be denoted by GR-LOC.

The operation of the passage to an arbitrary neighbourhood of the identity obviously defines some functor

$$\text{GR-DIFF} \to \text{GR-LOC}$$

(and also the functor GR_0-DIFF $\to$ GR-LOC) from the category GR-DIFF of all Lie groups (from the category GR_0-DIFF of all connected Lie groups) into the category GR-LOC of local Lie groups. That functor will be called a *localization functor*. The image of a Lie group G under the localization functor will sometimes be denoted by G_{loc}.

Lie groups are locally isomorphic if their localizations are isomorphic (as objects of the category GR-LOC).

The left-invariant vector fields and their Lie brackets are defined for local Lie groups in an obvious way. The collection $\mathfrak{l}(G)$ of all left-invariant vector fields on a local Lie group G is a Lie algebra called the *Lie algebra of a local Lie group G*. Just as for Lie groups, elements of the Lie algebra $\mathfrak{l}(G)$ are identified in a natural way with tangent vectors $A \in \mathsf{T}_e(G)$ and with one-parameter subgroups (or rather with *one-parameter local subgroups*, but this term is uncommon) of the local group G.

The resulting functor

$$\mathfrak{l}\colon \text{GR-LOC} \to \text{ALG}_f\text{-LIE}$$

will also be called a *Lie functor.*

Together with the Lie functors introduced above this functor enters the commutative diagram

$$\begin{tikzcd}
\text{GR-DIFF} \arrow[d] \arrow[dr, "2"] \arrow[drr, "4"] & & \\
\text{GR}_0\text{-DIFF} \arrow[r, "1"] \arrow[rr, bend right, "5"'] & \text{GR-LOC} \arrow[r, "3"] & \text{ALG}_f\text{-LIE}
\end{tikzcd}$$

in which the left vertical arrow represents the functor which associates the identity component with an arbitrary Lie group, arrows *1* and *2* represent localization functors and arrows *3*, *4* and *5* Lie functors.

We see that the functor GR-DIFF $\to$ ALG$_f$-LIE which is of primary interest to us breaks down into a composition of three functors: a functor GR-DIFF $\to$ GR$_0$-DIFF, a localization functor GR$_0$-DIFF $\to$ GR-LOC and a Lie functor GR-LOC $\to$ ALG$_f$-LIE for local Lie groups. Thus the study of the functor GR-DIFF $\to$ ALG$_f$-LIE reduces to the study of these three functors. The study of each of them requires peculiar methods and is virtually totally independent of the study of the others. Thus we have completely achieved our goal of separating local and global aspects. The local part of the problem is concentrated in the functor GR-LOC $\to$ ALG$_f$-LIE and the global part in the functors GR-DIFF $\to$ GR$_0$-DIFF and GR$_0$-DIFF $\to$ GR-LOC.

The functor GR-DIFF $\to$ GR$_0$-DIFF we have already considered in Lecture 1. As was proved there, any Lie group G is an extension of its component of the identity $H = G_e$ by means of a discrete group. Conversely, every extension G of a connected Lie group H by means of a discrete group is obviously a Lie group with $G_e = H$. In a first approximation this is sufficient to satisfactorily describe the functor GR-DIFF $\to$ GR$_0$-DIFF. The functor GR$_0$-DIFF $\to$ GR-LOC will be described in Lecture 10 and now we turn to the functor $\mathfrak{l}$: GR-LOC $\to$ ALG$_f$-LIE.

Lecture 4

The exponent of a linear differential operator · A formula for the values of smooth functions in the normal neighbourhood of the identity of a Lie group · A formula for the values of smooth functions on the product of two elements · The Campbell-Hausdorff series and Dynkin polynomials · The convergence of a Campbell-Hausdorff series · The reconstruction of a local Lie group from its Lie algebra · Operations in the Lie algebra of a Lie group and one-parameter subgroups · Differentials of internal automorphisms. The differential of an exponential mapping · Canonical coordinates · The uniqueness of the structure of a Lie group · Groups without small subgroups and Hilbert's fifth problem

Let M be any smooth manifold. In contrast to the foregoing we now assume that M is an *analytic* (class C^{ω}) manifold. Since every vector field X on M may be regarded as a linear differential operator acting on smooth functions, by analogy with the matrix case we may consider a linear operator

$$(1) \qquad e^X = E + X + \frac{X^2}{2!} + \cdots + \frac{X^n}{n!} + \cdots = \sum_{n=0}^{\infty} \frac{X^n}{n!},$$

where E is the identity operator and X^n designates an n-fold iteration of an operator X.

Of course, at this point we must define what is to be understood by the sum of an infinite series (1). In principle, to this end it is necessary to introduce into the space $\mathcal{O}(M)$ a topology (say given by some norm). For simplicity, however, we prefer a roundabout way here and will treat the convergence of series (4) in a "weak" sense. Namely, *we define*

the result $e^X f$ of applying the operator e^X to a function $f \in \mathcal{O}(M)$ by the formula

$$(2) \quad e^X f = f + Xf + \frac{X^2 f}{2!} + \cdots + \frac{X^n f}{n!} + \cdots = \sum_{n=0}^{\infty} \frac{X^n f}{n!},$$

where $X^n f = X(X^{n-1} f)$, and assume that this operator applies only to such functions for which series (2) (now a functional one) has a nonempty domain of convergence (which is taken to be the domain of the function $e^X f$).

The operator e^X will no longer be a differential operator. Namely, as shown later, it is generally induced by some diffeomorphism $\Phi\colon M \to M$, i.e. is of the form $f \mapsto f \circ \Phi$. This only requires that integral curves $t \mapsto \varphi_a(t)$ of the field X should be "long enough", viz. they should be defined for $| \quad | \leqslant 1$, and that the domain $W(f)$ of the function f should be "large enough", viz. that there should be points $a \in W(f)$ such that $\varphi_a(t) \in W(f)$ for $|t| \leqslant 1$. Then the function $e^x f$ will be defined for all such points a and expressed by the formula

$$(3) \qquad (e^X f)(a) = f(\varphi_a(1)).$$

Indeed, consider a function

$$F(t) = f(\varphi_a(t)).$$

Under the hypothesis, the function is defined and analytic for $|t| \leqslant 1$. It therefore can be expanded into a Taylor series

$$F(t) = \sum_{n=0}^{\infty} \frac{F^{(n)}(0)}{n!} t^n,$$

convergent for $|t| \leqslant 1$. On the other hand, since the curve $t \mapsto \varphi_a(t)$ is an integral curve of the field X, we have

$$F'(t) = \frac{df(\varphi_a(t))}{dt} = \frac{d\varphi_a(t)}{dt} f = X_{\varphi_a(t)} f = (Xf)(\varphi_a(t)).$$

This means that the function $F'(t)$ serves as the function $F(t)$ for the function Xf, from which an obvious induction yields that the function $F^{(n)}(t)$ serves as the function $F(t)$

for the function $X^n f$, i.e. that

$$F^{(n)}(t) = (X^n f)(\varphi_a(t)).$$

Therefore

$$F^{(n)}(0) = (X^n f)(\varphi_a(0)) = (X^n f)(a),$$

and hence

$$F(t) = \sum_{n=0}^{\infty} \frac{(X^n f)(a)}{n!} t^n = \sum_{n=0}^{\infty} \frac{(tX)^n f}{n!}(a) = (e^{tX} f)(a).$$

To complete the proof it remains to put $t = 1$. □

We shall apply the general formula (3) to left-invariant vector fields X on an analytic (or local) Lie group G and to functions f defined and analytic in some neighbourhood of the identity e of the group G. We take the identity e to be the point a. On denoting the point $\varphi_e(1)$ by $\exp X$ we rewrite (3) as follows for this case:

$$f(\exp X) = (e^X f)(e). \tag{4}$$

It is in this form that (3) will be used.

The corresponding one-parameter subgroup $t \mapsto \beta(t)$ is the integral curve $t \mapsto \varphi_e(t)$ for a left-invariant vector field X. Therefore $\exp X = \beta(1)$, and formula (4) holds for any functions f whose domain contains a segment $t \mapsto \beta(t)$, $|t| \leqslant 1$ of that subgroup.

By definition exp is a mapping of a vector space $\mathfrak{g} = \mathfrak{l}(G)$ into the group G such that $\exp 0 = e$. It obviously has the *property of naturalness*, i.e. for any homomorphism $\Phi: G \to H$ of Lie groups there exists a commutative diagram

$$\begin{tikzcd} \mathfrak{l}(G) \arrow[r, "\mathfrak{l}(\Phi)"] \arrow[d, "\exp"'] & \mathfrak{l}(H) \arrow[d, "\exp"] \\ G \arrow[r, "\Phi"] & H \end{tikzcd}$$

It follows immediately from the theorem on the smooth dependence of solutions of differential equations on the initial data that the mapping $\exp\colon \mathfrak{l}(G) \to G$ is smooth.

Statement A. *The mapping*

$$\exp\colon \mathfrak{l}(G) \to G$$

is a diffeomorphism at the point 0.

We prove this statement later on.

Definition 1. A neighbourhood $\mathring{U}$ of the null vector $0 \in \mathfrak{g}$ is said to be *normal* if:

(a) it has the *property of being starlike*, i.e. along with some vector X it contains all vectors of the form tX for $|t| \leqslant 1$;

(b) the mapping exp transforms $\mathring{U}$ diffeomorphically onto some neighbourhood U of the identity of the group G.

The neighbourhood U will also be called a *normal neighbourhood.*

According to Statement A there are arbitrarily small (contained in any preassigned neighbourhood) normal neighbourhoods (both of the vector $0 \in \mathfrak{g}$ and the identity $e \in G$).

By construction $\exp X = \beta(1)$, where β is a one-parameter subgroup which is an integral curve of the field X. But it is clear that for a field aX, where $a \in \mathbb{R}$, the curve $t \to \beta(at)$ is the integral curve which of course is also a one-parameter subgroup. It follows that $\exp(aX) = \beta(a)$ or, with a denoted by t, that

$$\exp(tX) = \beta(t).$$

This formula implies that $\beta\colon t \to \exp(tX)$, i.e. that *one-parameter subgroups* β *of the group* G *are the images of the line segments* $t \mapsto tX$ *when the exponent is mapped.*

It follows from condition (a) of Definition 1 that the condition on the domain of a function f, which is necessary (and sufficient) for formula (4) to be valid, is satisfied *a fortiori* if this domain is some normal neighbourhood U of the point e. Since any point in U is of the form $\exp X$, where $X \in \mathring{U}$, *formula* (4) *defines the function* f *on the entire neighbourhood* U.

With this in mind, we apply (4) to calculate the values $f(ab)$ of f on the product ab of two elements $a = \exp X$ and $b = \exp Y$ (assuming that $ab \in U$).

For a given element $a \in U$ the formula $f_a(b) = f(ab)$ defines (on some neighbourhood of the point e, contained in U which we may assume normal) a smooth function f_a. By (4) if $b = \exp Y$, then $f_a(b) = (e^Y f_a)(e)$.

On the other hand, since f_a is nothing but a composition $f \circ L_a$ of a left shift $L_a\colon b \mapsto ab$ and the function f, by virtue of left invariance of the field Y a formula

$$Yf_a = Yf \circ L_a = (Yf)_a$$

holds. But then $Y^n f_a = (Y^n f)_a$ for any $n \geqslant 0$ and therefore

$$e^Y f_a = (e^Y f)_a.$$

Consequently, if $a = \exp X$, then (we again apply formula (4))

$$f_a(b) = (e^Y f_a)(e) = (e^Y f)(a) = (e^X e^Y f)(e).$$

Since $f_a(b) = f(\exp X \cdot \exp Y)$ this proves that

$$f(\exp X \cdot \exp Y) = (e^X e^Y f)(e) \tag{5}$$

for any X and Y in the corresponding normal neighbourhood of the zero of an algebra $\mathfrak{g}$.

By definition (we neglect the question of convergence for the present)

$$e^X e^Y = \sum_{p=0}^{\infty} \frac{1}{p!} X^p \left(\sum_{q=0}^{\infty} \frac{1}{q!} Y^q \right) = \sum_{p,\, q=0}^{\infty} \frac{1}{p!q!} X^p Y^q.$$

On substituting this series in the logarithmic series

$$\ln Z = (Z - E) - \frac{(Z-E)^2}{2} + \ldots = \sum_{k=1}^{\infty} \frac{(-1)^{k-1}}{k} (Z-E)^k,$$

we obtain (considering that the operators X and Y do not in general commute) a formal series

$$\ln(e^X e^Y) = \sum_{k=1}^{\infty} \frac{(-1)^{k-1}}{k} \Bigg(\sum_{\substack{p,\, q=0 \\ p+q>0}}^{\infty} \frac{X^p Y^q}{p!q!} \Bigg)^k$$

$$= \sum_{k=1}^{\infty} \frac{(-1)^{k-1}}{k} \sum \frac{X^{p_1} Y^{q_1} \ldots X^{p_k} Y^{q_k}}{p_1!\, q_1! \ldots p_k!\, q_k!},$$

where in the internal sum the summation is taken over all possible collections $(p_1, \ldots, p_k, q_1 \ldots, q_k)$ of integral nonnegative numbers subject to the conditions

$$p_1 + q_1 > 0, \ \ldots, \ p_k + q_k > 0. \tag{6}$$

On putting

$$z_n(x, y) = \sum_{k=1}^{n} \frac{(-1)^{k-1}}{k} \sum \frac{x^{p_1} y^{q_1} \ldots x^{p_k} y^{q_k}}{p_1! \, q_1! \ldots p_k! \, q_k!}, \tag{7}$$

where in the internal sum along with condition (6) the exponents $p_1, \ldots, p_k, q_1, \ldots, q_k$ satisfy the condition

$$p_1 + \ldots + p_k + q_1 + \ldots + q_k = n, \tag{8}$$

we rewrite the series ln $(e^X e^Y)$ as follows:

$$\ln(e^X e^Y) = \sum_{n=1}^{\infty} z_n(X, Y). \tag{9}$$

This formal series is called a *Campbell-Hausdorff series.* From an algebraic standpoint, $z_n(x, y)$ is nothing but a polynomial in noncommuting, in general, variables x and y. We discuss this kind of polynomials in greater detail therefore.

Let x and y be some symbols and let $\mathbb{K}$ be any field. The ordinary polynomials in x and y over the field $\mathbb{K}$ are obtained from x, y and elements of $\mathbb{K}$ by applying the operations of addition and multiplication any number of times. Constructed in a similar way are also *noncommutative polynomials* in x and y over $\mathbb{K}$, the only difference being in that their multiplication is not assumed to be commutative (but as before $kf = fk$ for any polynomial f and any number $k \in \mathbb{K}$). They all form a unital algebra which will be denoted by $\mathbb{K}\langle x, y\rangle$. (A more formal definition of that algebra will be given in the next lecture.)

In the commutator algebra $[\mathbb{K}\langle x, y\rangle]$ of the algebra $\mathbb{K}\langle x, y\rangle$ *Lie polynomials* in x and y obtained from x and y by addition, multiplication by the elements of the field $\mathbb{K}$ and by the Lie operation $a, b \mapsto [a, b] = ab - ba$ are de-

fined in a natural way. It is clear that they make up a subalgebra of the Lie algebra $[\mathbb{K}\langle x, y\rangle]$ which contains the elements x, y and is contained in any other such subalgebra (i.e., to put it in general algebraic terms, generated by the elements x and y). We shall denote that subalgebra by $\mathfrak{l}\langle x, y\rangle$.

Every Lie polynomial $u \in \mathfrak{l}\langle x, y\rangle$ is at the same time a polynomial in $\mathbb{K}\langle x, y\rangle$ (it is sufficient to remove all Lie brackets by the rule $[a, b] = ab - ba$). In this capacity we shall denote the polynomial u by ιu. Formally, the mapping

$$\iota\colon \mathfrak{l}\langle x, y\rangle \to \mathbb{K}\langle x, y\rangle, \qquad u \mapsto \iota u,$$

is defined to be a linear mapping having the property that $\iota[a, b] = \iota a \cdot \iota b - \iota b \cdot \iota a$ for any elements $a, b \in \mathfrak{l}\langle x, y\rangle$. It is injective by definition.

If the field $\mathbb{K}$ has characteristic 0, then formula (7) defines some element $z_n(x, y)$ in $\mathbb{K}\langle x, y\rangle$.

Statement B. *There is a Lie polynomial* $\text{ڈ}_n(x, y)$ *such that*

$$\iota\,\text{ڈ}_n(x, y) = z_n(x, y).$$

Here the symbol ڈ reads "deh" (it is a form of the Arabic letter "dal").

We prove B later on.

Examples.

Let $n = 1$. It is obvious that

$$z_1(x, y) = x + y,$$

and therefore

$$\text{ڈ}_1(x, y) = x + y$$

(so that the Lie bracket is not involved in the construction of the polynomial $\text{ڈ}_1(x, y)$).

Let $n = 2$. For $k = 1$ the internal sum in formula (7) contains three terms $^1/_2 x^2$, xy and $^1/_2 y^2$, and for $k = 2$ it contains four terms x^2, xy, yx and y^2. Hence

$$z_2(x, y) = \frac{1}{2}xy - \frac{1}{2}yx,$$

and therefore

$$\mathfrak{z}_2(x, y)=\frac{1}{2}[x, y].$$

Similarly it can be checked that

$$z_3(x, y)=\frac{1}{12}x^2y+\frac{1}{12}yx^2+\frac{1}{12}xy^2 +\frac{1}{12}y^2x-\frac{1}{6}xyx-\frac{1}{6}yxy.$$

Here one can no longer see directly what sort of polynomial is $\mathfrak{z}_3(x, y)$ (and in general whether it exists). After some tests, however, one can see that

$$\mathfrak{z}_3(x, y)=\frac{1}{12}[x, [x, y]]+\frac{1}{12}[y, [y, x]].$$

With increasing n calculations become more and more complicated. Nevertheless it turns out to be possible to give for polynomials $\mathfrak{z}_n(x, y)$ an explicit formula similar to formula (7) for the polynomial $z_n(x, y)$. E. B. Dynkin was the first to indicate this formula. Therefore we call $\mathfrak{z}_n(x, n)$ *Dynkin polynomials.*

Notice that $\mathfrak{z}_n(x, n)$ *is a homogeneous polynomial of degree n in x and y*, i.e.

$$\mathfrak{z}_n(tx, ty) = t^n \mathfrak{z}_n(x, y)$$

for any t.

Since for vector fields (linear differential operators) the operation $X, Y \mapsto [X, Y]$ is also expressed by the formula $[X, Y] = XY - YX$, it follows from statement B that *for any operators $X, Y \in \mathfrak{l}(G)$ every operator $z_n(X, Y)$ belongs to the algebra $\mathfrak{l}(G)$.* So too does the operator $\ln(e^Xe^Y)$, if, of course, it is meaningful, i.e. if series (9) converges. We discuss therefore the question of convergence of that series or, to be more precise, the series

(10) $\mathfrak{z}_1(X, Y) + \mathfrak{z}_2(X, Y) + \dots + \mathfrak{z}_n(X, Y) + \dots$

composed of Lie polynomials $\mathfrak{z}_n(X, Y)$ in X and Y.

All terms of series (10) are in a finite-dimensional vector space $\mathfrak{g} = \mathfrak{l}(G)$ and therefore its convergence could in general be investigated by considering in $\mathfrak{g}$ an arbitrary (for example, Euclidean) norm.

However, the necessary estimates require rather detailed information about the structure of polynomials $\mathfrak{z}_n(x, y)$, which will be given only in the next lecture. So for the present we must be content with a roundabout way and return to series (9) the structure of whose terms is known but in going to which the advantage of finite-dimensionality is lost.

In accordance with our general treatment of convergence of operator series we shall understand the convergence of series (9) in a "weak" but somewhat stronger sense than above. Namely, we shall assume that the operator $\ln(e^X e^Y)$ defined by series (9) is applicable to a function $f \in \mathcal{O}(G)$ if the functional series

$$(11) \quad z_1(X, Y) f + z_2(X, Y) f + \ldots + z_n(X, Y) f + \ldots$$

converges in the domain of that function. The sum g of the series will be assumed to be the result of applying $\ln(e^X e^Y)$ to f.

Thus by this definition $W(g) = W(f)$ (whereas earlier $W(g) \subset W(f)$).

Assuming that some norm $\| \ \|$ is given in $\mathfrak{g}$ we now show that there *exists a number* $\delta_0 > 0$ *such that for* $\| X \| < \delta_0$ *and* $\| Y \| < \delta_0$ *the operator* $\ln(e^X e^Y)$ *is applicable to any function* $f \in \mathcal{O}(G)$. Since every element of G in the domain of f has a coordinate neighbourhood U with a compact closure $\bar{U}$, which is contained in this domain, it suffices to prove that *for any coordinate neighbourhood* U *with a compact closure* $\bar{U}$ *the operator* $\ln(e^X e^Y)$ *is defined on the vector space* $\mathcal{F}(\bar{U})$ *of all functions smooth on* $\bar{U}$.

To this end we notice that since the set $\bar{U}$ is compact, for any function $f \in \mathcal{F}(\bar{U})$ a number

$$\| f \| = \max\left(|f|, \left|\frac{\partial f}{\partial x^1}\right|, \ldots, \left|\frac{\partial f}{\partial x^n}\right| \right)$$

is defined, where $x^1, \ldots, x^n$ are the local coordinates in U (for, to be more precise, in a somewhat larger neighbourhood containing the closure $\bar{U}$ of U). Of course, the number $\| f \|$ depends on the choice of the coordinates $x^1, \ldots, x^n$, but this does not play any role in what follows. It can be checked in an obvious way that the functional $f \mapsto \| f \|$ thus

constructed is a norm on $\mathscr{F}(\bar{U})$. Since $Xf = X^i \frac{\partial f}{\partial x^i}$ and $|X^i| \leqslant \| X^i \|$ for all i, for every field $X \in \mathfrak{g}$ with $\| X \| < \delta$ there is an estimate

$$\| Xf \| \leqslant \delta \| f \|.$$

It can be derived from this by an obvious induction that if $\| X \| < \delta$ and $\| Y \| < \delta$, then for any exponents $p_1, \ldots, p_k, q_1, \ldots, q_k$ there is an estimate

$$\| X^{p_1} Y^{q_1} \ldots X^{p_k} Y^{q_k} f \| \leqslant \delta^n \| f \|,$$

where $n = p_1 + \ldots + p_k + q_1 + \ldots + q_k$. This means that series (11) is majorized (after being divided by $\| f \|$) by the series $\ln(e^X e^Y)$, with X and Y being replaced by a number δ and the coefficients replaced by their absolute values, i.e. it is majorized by the series obtained from the series

$$\sum_{n=1}^{\infty} \frac{(z-1)^n}{n} \tag{12}$$

by replacing z by

$$e^{2\delta} = \sum_{n=0}^{\infty} \frac{(2\delta)^n}{n!}.$$

Since (12) converges for $|z-1| < 1$, this majorizing series will converge for $|e^{2\delta} - 1| < 1$, i.e. for $\delta < \frac{\ln 2}{2}$. Hence for $\delta < \frac{\ln 2}{2}$ series (11) will uniformly converge in $\bar{U}$ to some smooth function, i.e. the operator $\ln(e^X e^Y)$ will be applicable to the function f. □

Since series (10) differs from series (9) only in notation (by definition $z_n(X, Y) = \mathfrak{z}_n(X, Y)$ for any fields $X, Y \in \mathfrak{g}$), this proves that for $\| x \| < \delta_0$, $\| Y \| < \delta_0$, where $\delta_0 = \frac{\ln 2}{2}$, series (10) converges in the same "weak" sense. But it is known that for the operator series whose terms belong to a finite-dimensional vector space the "weak" convergence coincides with the usual "strong" convergence. Hence *for* $\| X \| < \delta_0$ *and* $\| Y \| < \delta_0$ *series* (10) *converges* (in the usual sense).

Remark 1. Regardless of the reference to the general theorem on the coincidence of "strong" and "weak" convergences, we can prove the convergence of series (10) by considering an arbitrary system of local coordinates $x^1, \ldots, x^n$ at the point e of a group G. For $f = x^i$, $i = 1, \ldots, n$, series (11) turns into a series made up of components $z_n(X, Y)^i = \mathfrak{z}_n(X, Y)^i$ of vector fields $\mathfrak{z}_n(X, Y)$. Consequently, this series converges. Therefore so does the series made up of their values $\mathfrak{z}_n(X, Y)^i_e$ at e, i.e. of the coordinates $\left(\text{in the basis } \left(\frac{\partial}{\partial x^1}\right)_e, \ldots, \left(\frac{\partial}{\partial x^n}\right)_e\right)$ of vectors $\mathfrak{z}_n(X, Y)_e$). This means that the vector series

$$(13) \quad \mathfrak{z}_1(X_1, Y)_e + \mathfrak{z}_2(X, Y)_e + \ldots + \mathfrak{z}_n(X, Y)_e + \ldots$$

converges. Let $\mathfrak{z}(X, Y)_e$ be its sum and let $\mathfrak{z}(X, Y)$ be a left-invariant vector field assuming at e the value $\mathfrak{z}(X, Y)_e$. For any element $a \in G$ the series

$$\mathfrak{z}_1(X, Y)_a + \mathfrak{z}_2(X, Y)_a + \ldots + \mathfrak{z}_n(X, Y)_a + \ldots$$

made up of the values which take the terms of series (10) at the point e is obtained from series (13) by applying a linear operator dL_a, and therefore it converges to the vector $(dL_a(\mathfrak{z}(X, Y)_e) = \mathfrak{z}(X, Y)_a$. This precisely means that series (10) converges to $\mathfrak{z}(X, Y)$.

It is proved by calculus that if a function is expanded into a convergent power series, then that series is unique. It follows in particular that if the series for $\ln z$ is substituted into the series for e^z, then after collecting the like terms a series z results. In other words, the equation $e^{\ln z} = z$ holds not only for functions but also for formal series. It remains valid therefore also if z is replaced in it by say a series for $e^X e^Y$. This means that if z is replaced in the series for e^z by series (10) a series for $e^X e^Y$ is obtained. Since all the series here converge, this proves that

$$(14) \qquad e^{\mathfrak{z}(X, Y)} = e^X e^Y.$$

This formula holds for any elements X, Y of the algebra $\mathfrak{l}(G)$ for which $\| X \| < \delta_0$ and $\| Y \| < \delta_0$, where δ_0 is a sufficiently small number (according to the above investigation any $\delta_0 < \frac{\ln 2}{2}$ will do).

We now return to formula (5). It holds for any X and Y in some normal neighbourhood $\overset{\circ}{U}$ of zero of an algebra $\mathfrak{g} = \mathfrak{l}(G)$ which have the property that $\exp X \cdot \exp Y \in U = \exp \overset{\circ}{U}$. In particular, there is a δ_1 such that for any positive $\delta < \delta_1$ formula (5) holds for $\| X \| < \delta$ and $\| Y \| < \delta$. Assuming, in addition, that $\delta < \delta_0$ formula (5) can be rewritten as follows:

$$f(\exp X \cdot \exp Y) = (e^Z f)(e), \text{ where } Z = \mathfrak{Z}(X, Y).$$

Now notice that the element Z of $\mathfrak{l}(G)$ is obviously continuously dependent on its elements X and Y, so that in particular $Z \to 0$ when $X \to 0$ and $Y \to 0$. Therefore, with a sufficiently small δ the field Z satisfies formula (4) by which

$$(e^Z f)(e) = f(\exp Z).$$

Thus if $\| X \| < \delta$ and $\| Y \| < \delta$, where $\delta > 0$ is sufficiently small, then

$$f(\exp X \cdot \exp Y) = f(\exp Z)$$

for every smooth function f defined at the points $\exp X \cdot \exp Y$ and $\exp Z$. In particular, it is true when f is one of the coordinates $x^1, \ldots, x^n$ at e. Thus all the coordinates $x^1, \ldots, x^n$ assume equal values at $\exp X \cdot \exp Y$ and $\exp Z$, which is possible only when

$$\exp X \cdot \exp Y = \exp Z.$$

To sum up, we obtain the following theorem, which was the main goal of all the preceding arguments.

Theorem 1. *The identity element e of an analytic (or local) Lie group has a neighbourhood U which possesses the following properties:*

(a) *there is a $\delta > 0$ such that every point of U can be uniquely represented as* $\exp X$, *where $X \in \mathfrak{l}(G)$ and $\| X \| < \delta$;*

(b) *for any two points* $\exp X$ *and* $\exp Y$ *of U in $\mathfrak{l}(G)$ there exists an element Z such that*

$$\exp X \cdot \exp Y = \exp Z; \tag{15}$$

(c) *that element Z is the sum $\mathfrak{Z}(X, Y)$ of series* (10) *whose terms are Dynkin polynomials $\mathfrak{Z}_n(X, Y)$ in X and Y.* □

The theorem implies that a (local) Lie group G has a part in which multiplication is uniquely reconstructed (by for-

mula (15)) from the Lie algebra $\mathfrak{l}(G)$. Consequently, *two (analytic) local Lie groups with isomorphic Lie algebras are isomorphic* (more precisely, their germs are isomorphic). In that sense we may say that *the Lie functor*

$$L\colon \text{GR-LOC} \to \text{ALG}_f\text{-LIE}$$

is invertible to within an isomorphism.

A more precise statement will be obtained in Lecture 6.

Using Theorem 1 it is easy to solve the problem we have put off above of interpreting the operations of the algebra $\mathfrak{g} = \mathfrak{l}(G)$ in terms of one-parameter subgroups.

If a basis $e_1, \ldots, e_n$ is arbitrarily chosen in the vector space $\mathfrak{g}$, then for any normal neighbourhood U of the identity of the group G the composition h of a diffeomorphism $\exp^{-1}$: $U \to \overset{\circ}{U}$ with a restriction to $\overset{\circ}{U}$ of the corresponding coordinate isomorphism $\mathfrak{g} \to \mathbb{R}^n$ will be a diffeomorphism of U onto some open set of the space $\mathbb{R}^n$, i.e. the pair (U, h) will be a chart on the Lie group G. The corresponding local coordinates are called *normal coordinates*. Thus if $a = \exp X$ and $X = x^1e_1 + \ldots + x^ne_n$, then the numbers $x^1, \ldots, x^n$ are the normal coordinates of a point $a \in U$.

A one-parameter subgroup $t \mapsto \exp(tX)$ corresponding to an element $X \in \mathfrak{g}$ (i.e., if X is interpreted as a left-invariant vector field, an integral curve of that field passing for $t = 0$ through the point e, and, if X is interpreted as a vector of the tangent space $\mathsf{T}_e(G)$, a one-parameter subgroup having a tangent vector X for $t = 0$) will be denoted by β_X.

Proposition 1. *For any $X \in \mathfrak{g}$ and any $k \in \mathbb{R}$ an element $kX \in \mathfrak{g}$ (interpreted as the element of space $\mathsf{T}_e(G)$) is a tangent vector to a curve for $t = 0$*

$$t \mapsto \beta_X(kt). \tag{16}$$

For any $X, Y \in \mathfrak{g}$ the element $X + Y \in \mathfrak{g}$ is (in the same interpretation) a tangent vector to a curve for $t = 0$

$$t \mapsto \beta_X(t)\,\beta_Y(t) \tag{17}$$

and the element $[X, Y] \in \mathfrak{g}$ is a tangent vector to a curve for $t = 0$

$$t \mapsto \beta_X(\sqrt{t})\beta_Y(\sqrt{t})\,\beta_X(\sqrt{t})^{-1}\,\beta_Y(\sqrt{t})^{-1}. \tag{18}$$

Proof. The first statement is obvious since curve (16), i.e. the curve $t \mapsto \exp(ktX)$, is nothing but a one-parameter subgroup β_{kX}.

To prove the second statement notice that since $\mathfrak{H}_n(tX, tY) = t^n \mathfrak{H}_n(X, Y)$ and $\mathfrak{H}_1(X, Y) = X + Y$, we have

$$\mathfrak{H}(tX, tY) = t(X + Y) + O(t^2),$$

where $O(t^2)$ stands for the terms of degree $\geqslant 2$ in t. Curve (17) therefore is of the form

$$t \mapsto \exp(t(X + Y) + O(t^2))$$

and hence, in normal coordinates (defined by an arbitrary basis of the Lie algebra $\mathfrak{g}$) it is given by the functions

$$x^i(t) = t(X^i + Y^i) + O(t^2).$$

Consequently, for $t = 0$ its tangent vector has coordinates

$$\left.\frac{dx^i(t)}{dt}\right|_{t=0} = X^i + Y^i$$

and hence coincides with the vector $X + Y$.

Similarly, since

$$\begin{aligned}(\exp X)\cdot(\exp Y)\cdot(\exp X)^{-1}\cdot(\exp Y)^{-1} &= \exp X\cdot\exp Y\cdot\exp(-X)\cdot\exp(-Y)\\ &= \exp(\mathfrak{H}(X, Y))\exp(\mathfrak{H}(-X, -Y))\\ &= \exp\mathfrak{H}(\mathfrak{H}(X, Y), \mathfrak{H}(-X, -Y))\end{aligned}$$

and

$$\begin{aligned}\mathfrak{H}(\mathfrak{H}(X, Y), \mathfrak{H}(-X, -Y)) &= \mathfrak{H}(X, Y) + \mathfrak{H}(-X, -Y)\\ &+\frac{1}{2}[\mathfrak{H}(X, Y), \mathfrak{H}(-X, -Y)] + \dots\\ &= \left\{(X+Y) + \frac{1}{2}[X, Y] + \dots\right\}\\ &+\left\{(-X-Y) + \frac{1}{2}[-X, -Y] + \dots\right\}\\ &+\frac{1}{2}[X+Y+\dots, -X-Y+\dots] + \dots = \frac{1}{2}[X, Y]\\ &+\frac{1}{2}[X, Y] + \frac{1}{2}[X, -Y] + \frac{1}{2}[Y, -X] + \dots\\ &= [X, Y] + \dots,\end{aligned}$$

curve (18) is of the form

$$t \mapsto \exp([\sqrt{t}\, X, \sqrt{t}\, Y] + O(t^{3/2})) = \exp(t\,[X, Y] + O(t^{3/2}))$$

and is hence, in normal coordinates, given by the functions

(19) $\quad x^i(t) = t\,[X, Y]^i + O(t^{3/2}), \qquad i = 1, \ldots, n.$

Consequently,

$$\left.\frac{dx^i(t)}{dx}\right|_{t=0} = [X, Y]^i$$

and hence a tangent vector to curve (18) for $t = 0$ is the vector $[X, Y]$. □

Remark 2. Note that while curve (16) is a one-parameter subgroup curves (17) and (18) *are not*. Moreover, curve (18) is defined only for $t \geqslant 0$, so that we cannot speak about its tangent vector for $t = 0$. Therefore we must give an ad hoc definition of a tangent vector to curve (18) for $t = 0$. We shall take as that vector the limit for $t \to 0$ of tangent vectors to curve (18) for $t > 0$. It follows from formulas (19) that this limit exists and is $[X, Y]$.

Remark 3. It is also useful to have in mind that in formulas (17) and (18) one-parameter subgroups β_X and β_Y can be replaced by arbitrary curves α_X: $t \mapsto \alpha_X(t)$ and α_Y: $t \mapsto \alpha_Y(t)$ for $t = 0$ passing through the point e and having tangent vectors X and Y. Indeed, with $|t|$ sufficiently small, vectors $\mathring{\alpha}_X(t) = \exp^{-1} \alpha_X(t)$ and $\mathring{\alpha}_Y(t) = \exp^{-1} \times \alpha_Y(t)$ are defined in $\mathfrak{g}$ and for these vectors we have

$$\mathring{\alpha}_X(t) = tX + O(t^2), \qquad \mathring{\alpha}_Y(t) = tY + O(t^2)$$

and hence

$$\mathfrak{Z}(\mathring{\alpha}_X(t), \mathring{\alpha}_Y(t)) = t(X + Y) + O(t^2).$$

Therefore for $t = 0$ a tangent vector to, say, a curve

$$t \mapsto \alpha_X(t)\, \alpha_Y(t) = \exp \mathfrak{Z}(\mathring{\alpha}_X(t), \mathring{\alpha}_Y(t))$$

is the vector $X + Y$.

Theorem 1 also allows one to calculate the differential of an arbitrary interior automorphism.

For every element a of a Lie group G the differential $(d\Phi_a)_e = \mathfrak{l}(\Phi_a)$ of the corresponding interior automorphism

$\Phi_a: x \mapsto axa^{-1}, x \in G$, is denoted by Ad (a). This automorphism is a linear invertible mapping

$$\mathrm{Ad}\,(a): \mathfrak{g} \to \mathfrak{g}$$

of the vector space $\mathfrak{g} = \mathfrak{l}\,(G)$ onto itself. Since $\Phi_a = L_a \circ R_{a^{-1}}$, we have (in the interpretation $\mathfrak{g} = \mathsf{T}_e\,(G)$)

$$\mathrm{Ad}\,(a) = (dL^{-1}_a)_{a^{-1}} \circ (dR_{a^{-1}})_e.$$

It is clear that the mapping

$$\mathrm{Ad}: a \mapsto \mathrm{Ad}\,(a)$$

is a homomorphism of a Lie group G into the Lie group Aut $\mathfrak{g}$ of all nonsingular linear operators of the vector space $\mathfrak{g}$. That homomorphism is called an *adjoint representation of G*.

The differential $(d\,\mathrm{Ad})_e = \mathfrak{l}\,(\mathrm{Ad})$ of the homomorphism Ad at point e is a linear mapping of the vector space $\mathfrak{g} = \mathfrak{l}\,(G)$ into the vector space End $\mathfrak{g} = \mathfrak{l}$ (Aut $\mathfrak{g}$) of all linear operators of $\mathfrak{g}$. On the other hand, we know from Lecture 3 that for any Lie algebra $\mathfrak{g}$ there is a linear mapping ad: $\mathfrak{g} \to$ End $\mathfrak{g}$ acting by the formula

$$\mathrm{ad}\, X: Y \mapsto [X, Y], \qquad X, Y \in \mathfrak{g}.$$

Proposition 2. *We have*

$$\mathfrak{l}\,(\mathrm{Ad}) = \mathrm{ad}.$$

Proof (cf. the proof of Proposition 1). Since

$$\begin{aligned}\daleth\,(\daleth(X, Y), -X) &= \daleth\left(X+Y+\frac{1}{2}[X, Y]+\ldots, -X\right)\\ &= Y+\frac{1}{2}[X, Y]+\frac{1}{2}[Y, -X]+\ldots\\ &= Y+[X, Y]+\ldots,\end{aligned}$$

where the dots designate terms of at least the third degree in X and Y, we have

$$\begin{aligned}(\exp X)\,(\exp Y)\,(\exp X)^{-1} &= \exp \daleth\,(\daleth\,(X, Y), -X)\\ &= \exp\,(Y + [X, Y] + \ldots)\end{aligned}$$

and hence

$$\begin{aligned}\Phi_{\beta_X(s)}\,(\beta_Y\,(t)) &= (\exp\,(sX))\,(\exp\,(tY))\,(\exp\,(sX))^{-1}\\ &= \exp\,(tY + st\,[X, Y] + \ldots),\end{aligned}$$

where the dots designate terms of at least the third degree in s and t. Consequently, the normal coordinates of the vector

$$(d\Phi_{\beta_X(s)})_e Y = (d\Phi_{\beta_X(s)})\left(\left(\frac{d\beta_Y(t)}{dt}\right)_{t=0}\right) = \left(\frac{d}{dt}\Phi_{\beta_X(s)}(\beta_Y(t))\right)\Big|_{t=0}$$

are

$$\frac{d}{dt}(tY^i + st[X, Y]^i + \ldots)\Big|_{t=0} = Y^i + s[X, Y]^i + \ldots,$$

where the last dots designate terms of at least the second degree in s and hence

$$(d\Phi_{\beta_X(s)})_e Y = Y + s[X, Y] + \ldots$$

Since

$$(d\,\mathrm{Ad})_e X = (d\,\mathrm{Ad})_e\left(\frac{d\beta_X(s)}{ds}\Big|_{s=0}\right) = \frac{d}{ds}\mathrm{Ad}(\beta_X(s))\Big|_{s=0}$$
$$= \lim_{s\to 0}\frac{\mathrm{Ad}(\beta_X(s)) - \mathrm{Ad}(e)}{s} = \lim_{s\to 0}\frac{(d\Phi_{\beta_X(s)})_e - E}{s},$$

it follows that

$$((d\,\mathrm{Ad})_e X)\,Y = \lim_{s\to 0}\frac{(d\Phi_{\beta_X(s)})_e Y - Y}{s}$$
$$= \lim_{s\to 0}([X, Y] + \ldots) = [X, Y] = (\mathrm{ad}\,X)\,Y. \quad \square$$

Corollary. *For any element $X \in \mathfrak{g}$ we have*

$$\mathrm{Ad}(\exp X) = e^{\mathrm{ad}\,X}.$$

Proof. The formulas

$$t \mapsto \mathrm{Ad}\,(t \exp X) \text{ and } \quad t \mapsto e^{t\,\mathrm{ad}\,X}$$

give one-parameter subgroups of the Lie group $\mathrm{Aut}\,\mathfrak{g}$ which have the same tangent vector for $t = 0$

$$(d\,\mathrm{Ad})_e X = \mathrm{ad}\,X$$

and hence coincide for all t. $\square$

Another example of using Theorem 1 arises from considering in the Lie algebra $\mathfrak{g} = \mathfrak{l}(G)$ a smooth curve $t \mapsto X(t)$. For any $s \in \mathbb{R}$ the mapping $t \mapsto \exp(sX(t))$ is some curve in G passing for $t = 0$ through a point $a(s) = \exp(sX)$, where $X = X(0)$. Let

$$A(s) = \frac{d}{dt}\exp(sX(t))\Big|_{t=0}$$

be a tangent vector to that curve at $a(s)$. On translating that vector by means of the differential $(dR_{a(s)^{-1}})_{a(s)}$ to the point e we obtain a vector $\mathfrak{g} = \mathsf{T}_e(G)$

$$B(s) = (dR_{a(s)^{-1}})_{a(s)}A(s).$$

The mapping $s \mapsto B(s)$ is a smooth curve in $\mathfrak{g}$ and hence for any s its tangent vector $B'(s)$ is defined. It turns out that

$$B'(s) = \operatorname{Ad}(a(s))\,Y, \tag{2}$$

where $Y = X'(0)$. Indeed, by definition of the action of the differential of a smooth mapping upon the tangent vectors to the curves

$$\begin{aligned} B(s) &= \frac{d}{dt}(R_{a(s)^{-1}}(\exp(sX(t))))\Big|_{t=0} \\ &= \frac{d}{dt}(\exp(sX(t)))\exp(-sX)\Big|_{t=0} \end{aligned}$$

and hence according to Remark 3

$$\begin{aligned} B(s+\Delta s) - B(s) &= \frac{d}{dt}((\exp(sX(t))\exp(-sX))^{-1} \\ &\quad \times (\exp((s+\Delta s)X(t))\exp(-(s+\Delta s)X))|_{t=0} \\ &= \frac{d}{dt}(\exp(sX)\exp(-sX(t)) \\ &\quad \times \exp((s+\Delta s)X(t))\exp(-(s+\Delta s)X))|_{t=0} \\ &= \frac{d}{dt}(a(s)\exp(\Delta sX(t))\,a(s+\Delta s)^{-1}) \\ &= (dL_{a(s)} \circ dR_{a(s+\Delta s)^{-1}})\frac{d}{dt}(\exp(\Delta sX(t)))\Big|_{t=0}. \end{aligned}$$

Therefore

$$B'(s) = \lim_{\Delta s \to 0} \frac{B(s+\Delta s) - B(s)}{\Delta s}$$

$$= (dL_{a(s)} \circ dR_{a(s)^{-1}}) \lim_{\Delta s \to 0} \frac{\left.\frac{d}{dt}(\exp(\Delta s X(t)))\right|_{t=0}}{\Delta s}$$

$$= \mathrm{Ad}\,(a(s)) \lim_{\Delta s \to 0} \frac{\left.\frac{d}{dt}(\exp(\Delta s X(t)))\right|_{t=0}}{\Delta s}$$

and hence for equation (20) to be proved it suffices to prove that

$$\lim_{\Delta s \to 0} \frac{\left.\frac{d}{dt}(\exp(\Delta s X(t)))\right|_{t=0}}{\Delta s} = Y.$$

But it is obvious, since in normal coordinates corresponding to a basis $e_1, \ldots, e_n$ of the vector space $\mathfrak{g}$ the point $\exp(\Delta s X(t))$ has coordinates $\Delta s X^i(t)$, where $X^i(t)$ are the coordinates of a vector $X(t)$ in the basis $e_1, \ldots, e_n$ and hence the vector

$$\lim_{\Delta s \to 0} \frac{\left.\frac{d}{dt}(\exp(\Delta s X(t))\right|_{t=t_0}}{\Delta s}$$

has in the basis $e_1, \ldots, e_n$ coordinates $\frac{dX^i(0)}{dt}$, i.e. the same coordinates as the vector $X'(0) = Y$. □

The linear operator $\mathrm{Ad}\,(a(s))$ involved in formula (20) can be rewritten as follows:

$$\mathrm{Ad}\,(a(s)) = \mathrm{Ad}\,(\exp(sX)) = e^{s\,\mathrm{ad}\,X}$$

$$= E + s\,\mathrm{ad}\,X + \ldots + s^n \frac{(\mathrm{ad}\,X)^n}{n!} + \cdots$$

Integrating this operator identity with respect to s between 0 and 1 we obtain an identity

$$\int_0^1 \mathrm{Ad}\,(a(s))\,ds = \frac{e^{\mathrm{ad}\,X} - E}{\mathrm{ad}\,X},$$

where by $\frac{e^{\mathrm{ad}\, X}-E}{\mathrm{ad}\, X}$ is meant the sum of an operator series

$$E+\frac{\mathrm{ad}\, X}{2!}+\cdots+\frac{(\mathrm{ad}\, X)^n}{(n+1)!}+\cdots$$

obtained from the power series for the function $\frac{e^z-1}{z}$ by substituting the operator ad X for z. For the vector $B(1)$, it follows from formula (20) that

$$B(1)=\int_0^1 B'(s)\,ds=\frac{e^{\mathrm{ad}}-E}{\mathrm{ad}\, X}\,Y.$$

Since by definition

$$\begin{aligned} B(1)&=(dR_{a(1)^{-1}})_{a(1)}\frac{d}{dt}\exp X(t)\Big|_{t=0}\\ &=(dR_{\exp(-X)})_{\exp X}\,\frac{d}{dt}\exp X(t)\Big|_{t=0}\\ &=\frac{d}{dt}(\exp X(t)\exp(-X))\Big|_{t=0}, \end{aligned}$$

this proves that

$$\frac{d}{dt}(\exp X(t)\exp(-X))\Big|_{t=0}=\frac{e^{\mathrm{ad}\, X}-E}{\mathrm{ad}\, X}\,Y.$$

Going over to normal coordinates we immediately see that for the vector $Z(t)\in\mathfrak{g}$ satisfying the relation $\exp X(t)\times \exp(-X)=\exp Z(t)$, we have

$$Z'(0)=\frac{e^{\mathrm{ad}\, X}-E}{\mathrm{ad}\, X}\,Y$$

which yields

$$Z(t)=t\,\frac{e^{\mathrm{ad}\, X}-E}{\mathrm{ad}\, X}\,Y+O(t^2).$$

Going back to $\exp Z(t)$ and assuming $X(t)=X+tY$ we see that we have proved

Proposition 3. *For any elements $X, Y\in\mathfrak{g}$ we have*

$$\exp(X+tY)\exp(-X)=\exp\left(t\,\frac{e^{\mathrm{ad}\, X}-E}{\mathrm{ad}\, X}\,Y+O(t^2)\right).\ \square$$

For every element $X \in \mathfrak{g}$ the differential $(d\exp)_X$ at point X of a smooth mapping $\exp: \mathfrak{g} \to G$ is, by virtue of identification $\mathsf{T}_X(\mathfrak{g}) = \mathfrak{g}$, a linear mapping $\mathfrak{g} \to \mathsf{T}_a(G)$, where $a = \exp X$. Its composition with the mapping $(dR_a)_e^{-1}$: $\mathsf{T}_a(G) = \mathsf{T}_e(G) = \mathfrak{g}$ therefore is a mapping from $\mathfrak{g}$ into $\mathfrak{g}$.

Corollary 1. *An expression*

$$(dR_a)_e^{-1} \circ (d\exp)_X = \frac{e^{\operatorname{ad} X} - E}{\operatorname{ad} X}, \quad a = \exp X$$

holds.

Proof. Let $Y \in \mathfrak{g}$. Since $\left.\frac{d(X+tY)}{dt}\right|_{t=0} = Y$, we have

$$((dR_a^{-1})_e \circ (d\exp)_X Y = \frac{d}{dt}(\exp(X+tY)\exp(-X))\Big|_{t=0}$$
$$= \frac{d}{dt}\left(t\frac{e^{\operatorname{ad} X} - E}{\operatorname{ad} X} Y + O(t^2)\right|_{t=0}$$
$$= \frac{e^{\operatorname{ad} X} - E}{\operatorname{ad} X} Y. \ \square$$

Corollary 2. *The mapping* $\exp: \mathfrak{g} \to G$ *is a diffeomorphism at point* $X \in \mathfrak{g}$ *if and only if not a single characteristic root of the operator* $\operatorname{ad} X$ *is of the form* $2m\pi i$.

Proof. A mapping exp is a diffeomorphism at point X if and only if its differential $(d\exp)_X$ at that point is an isomorphism and the operator $\operatorname{ad} X$ has characteristic roots of the form $2m\pi i$, if and only if the operator $e^{\operatorname{ad} X} - E$, and hence the operator $\frac{e^{\operatorname{ad} X} - E}{\operatorname{ad} X}$, is singular. $\square$

We stress that we have only proved all these results modulo statements A and B. Our immediate goal therefore should be to prove these statements.

We first prove statement A, and do so in a somewhat more general form.

Suppose a linear space $\mathfrak{g} = \mathfrak{l}(G)$ is decomposed into a direct sum

(21) $$\mathfrak{g} = \mathcal{A} \otimes \mathcal{B}$$

of two subspaces $\mathcal{A}$ and $\mathcal{B}$. We define a mapping

(22) $$\Phi: \mathfrak{g} \to G$$

assuming for any $X \in \mathfrak{g}$

$$\Phi(X) = \exp A \cdot \exp B,$$

where $A \in \mathscr{A}$ and $B \in \mathscr{B}$ are components of a vector $X \in \mathfrak{g}$ in decomposition (21). Clearly that mapping is smooth and sends the zero $0 \in \mathfrak{l}(G)$ to the identity $e \in G$. We find the differential

$$(d\Phi)_0\colon \mathsf{T}_0(\mathfrak{g}) \to \mathsf{T}_e(G)$$

of the mapping at the point 0.

Let

$$l\colon \mathfrak{g} \to \mathsf{T}_0(\mathfrak{g})$$

be a natural isomorphism sending a vector $X \in \mathfrak{g}$ to a tangent vector to a curve $t \mapsto tX$ at point 0. The mapping Φ sends that curve to a curve

$$t \mapsto \exp tA \cdot \exp tB = \exp \mathfrak{H}(tA, tB) \tag{23}$$

and hence its differential $(d\Phi)_0$ sends the vector $l(X)$ to a tangent vector to curve (23) at point e. This means that for any function $f \in \mathcal{O}_e(G)$

$$[((d\Phi)_0 \circ l)(X)]f = \left.\frac{df(\exp \mathfrak{H}(tA, tB))}{dt}\right|_{t=0}$$

and hence (see formula (4))

$$[((d\Phi)_0 \circ l)(X)]f = \left.\frac{d(e^{\mathfrak{H}(tA, tB)}f)(e)}{dt}\right|_{t=0}.$$

But

$$\begin{aligned} e^{\mathfrak{H}(tA, tB)}f &= (E + \mathfrak{H}(tA, tB) + O(t^2))f \\ &= f + t(A+B)f + O(t^2), \end{aligned}$$

and therefore

$$\left.\frac{d(e^{\mathfrak{H}(tA, tB)}f)(e)}{dt}\right|_{t=0} = ((A+B)f)(e) = (Xf)(e) = X_e f.$$

Consequently,

$$((d\Phi)_0 \circ l)(X) = X_e,$$

i.e.

$$(d\Phi)_0 \circ l = i,$$

where i is an isomorphism $X \to X_e$ of the vector space $\mathfrak{g} = \mathfrak{l}(G)$ onto the vector space $\mathsf{T}_e(G)$.

Since i and l are isomorphisms, it follows that the mapping $(d\Phi)_0$ is also an isomorphism. By virtue of the theorem on étale (locally diffeomorphic) mappings this proves the following proposition:

Proposition 4. *Mapping* (22) *is a diffeomorphism at* $0 \in \mathfrak{g}$. □

For $\mathfrak{g} = \mathscr{A}$ (and $\mathscr{B} = 0$) we obtain statement A which is thus completely proved.

By Proposition 4 the point $0 \in \mathfrak{g}$ has an arbitrary small starlike neighbourhood $\mathring{U}$ on which mapping (22) is its diffeomorphism onto some neighbourhood U of the identity $e \in G$.

Definition 2. Neighbourhoods $\mathring{U}$ and U having this property are called *canonical neighbourhoods* (of the points $0 \in \mathfrak{g}$ and $e \in G$ respectively) corresponding to a given direct sum (21).

By choosing arbitrary bases in subspaces $\mathscr{A}$ and $\mathscr{B}$ we obtain some basis of $\mathfrak{g}$. The composition h of a diffeomorphism $\Phi^{-1}: U \to \mathring{U}$ and a restriction to $\mathring{U}$ of the corresponding coordinate isomorphism $\mathfrak{g} \to \mathbb{R}^n$ is a diffeomorphism of U onto some open set of the space $\mathbb{R}^n$, i.e. a pair (U, h) is some chart on G.

Charts of this form are called *canonical charts* corresponding to decomposition (21) and the corresponding local coordinates $x^1, \ldots, x^n$ are called *canonical coordinates.*

It is clear that these definitions (together with Proposition 4) are all automatically carried over to the case of the decomposition

$$\mathfrak{g} = \mathscr{A}_1 \oplus \cdots \oplus \mathscr{A}_m \tag{24}$$

of a vector space $\mathfrak{g}$ into a direct sum of any number of subspaces.

If in (21) $\mathscr{A} = \mathfrak{g}$ and $\mathscr{B} = 0$, i.e. if in decomposition (24) $m = 1$, then canonical neighbourhoods coincide with normal neighbourhoods in the sense of Definition 1 and canonical coordinates coincide with normal coordinates.

Another extreme case arises for $m = n$, when spaces $\mathcal{A}_1, \ldots, \mathcal{A}_m$ are all one-dimensional (i.e. when decomposition (24) is defined by the choice in $\mathfrak{g}$ of some basis). The corresponding canonical coordinates are called *canonical coordinates of the second kind* (whereas normal coordinates are the *canonical coordinates of the first kind*).

Notice that canonical coordinates of the first and the second kind are given by an arbitrary basis of the vector space $\mathfrak{g}$.

Using canonical coordinates we can easily prove the following important proposition:

Proposition 5. *Any continuous homomorphism* $\Phi\colon H \to G$ *of Lie groups (i.e. their homomorphism as that of topological groups) is a smooth mapping (their homomorphism as that of Lie groups).*

Proof. Let $a \in H$ and $g \in \mathcal{O}_{\Phi(a)}(G)$. We have to prove that the function $g \circ \Phi$ defined in the neighbourhood of a point a is a smooth function at that point, i.e. it belongs to $\mathcal{O}_a(H)$. But since Φ is a homomorphism

$$\Phi = L_{\Phi a}^{-1} \circ \Phi \circ L_a.$$

Therefore, since the mapping L_a and the function $f = g \circ L_{\Phi a}^{-1}$ are smooth, it suffices to prove that for any function $f \in \mathcal{O}_e(G)$ the function $f \circ \Phi$ is smooth in the neighbourhood of the identity $e \in H$, i.e. that the mapping Φ is smooth at e.

Consider first the case where H is the additive group $\mathbb{R}$ of real numbers. Let U be a normal neighbourhood (a canonical group of the first kind) of the identity e in a group G and let $x^1, \ldots, x^n$ be the corresponding normal coordinates. Suppose further $\varepsilon > 0$ is a number such that $\Phi(t) \in U$, when $|t| < \varepsilon$. If $0 < t < \varepsilon$ and $0 < |r| < s$, where r and s are integers, then

$$\Phi\left(\frac{r}{s}t\right) = \Phi\left(\frac{t}{s}\right)^r \quad \text{and} \quad \Phi(t) = \Phi\left(\frac{t}{s}\right)^s.$$

On the other hand, since the coordinates $x^1, \ldots, x^n$ are normal, for any $i = 1, \ldots, n$ of any element $a \in U$ and any s such that $a^s \in U$, we have

$$x^i(a^s) = sx^i(a)$$

(it suffices to notice that if $a = \exp A$, then $a^s = \exp(sA)$). Consequently,

$$(x^i \circ \Phi)\left(\frac{r}{s}\,t\right) = r\cdot(x^i \circ \Phi)\left(\frac{t}{s}\right)$$

and

$$(x^i \circ \Phi)(t) = s\cdot(x^i \circ \Phi)\left(\frac{t}{s}\right).$$

Therefore

$$(x^i \circ \Phi)\left(\frac{r}{s}\,t\right) = \frac{r}{s}\cdot(x^i \circ \Phi)(t).$$

Since the mapping Φ is continuous, a similar equation

$$(x^i \circ \Phi)(\alpha t) = \alpha\cdot(x^i \circ \Phi)(t)$$

is true also for any real α, $|\alpha| < 1$. This means that functions $x^i \circ \Phi$ are linear. Thus Φ is given in local coordinates by linear and hence analytic functions. Therefore it is smooth.

Now let H be an arbitrary group. Choose an arbitrary basis $Y_1, \ldots, Y_n$ in its Lie algebra $\mathfrak{h}$. Then for any $i = 1, \ldots, n$ the mapping $t \mapsto \Phi(\exp tY_1)$ will be a continuous and hence, according to the foregoing, smooth homomorphism $\mathbb{R} \to G$, i.e. a one-parameter subgroup of a group G. There are, therefore, elements $X_1, \ldots, X_n$ in a Lie algebra $\mathfrak{g}$ of G such that

$$\Phi(\exp tY_i) = \exp tX_i$$

for any $i = 1, \ldots, n$. Since Φ is a homomorphism, it follows that for any numbers $t^1, \ldots, t^n \in \mathbb{R}$

$$\Phi(\exp t^1Y_1 \ldots \exp t^nY_n) = \exp t^1X_1 \ldots \exp t^nX_n.$$

It is clear that the element $\exp t^1X_1 \ldots \exp t^nX_n$ of G depends smoothly on $t^1, \ldots, t^n$, i.e. its local coordinates $x^1, \ldots, x^n$ (in an arbitrary chart) are smooth functions $x^1(t), \ldots, x^n(t)$ of $t = (t^1, \ldots, t^n)$. But by definition numbers $t^1, \ldots, t^n$ are (in some neighbourhood of the identity of the group H) nothing but canonical coordinates of the second kind defined by a given basis of the algebra $\mathfrak{h}$. Therefore functions $x^1(t), \ldots, x^n(t)$ are the functions giving a mapping Φ in local coordinates $t^1, \ldots, t^n$ and $x^1, \ldots, x^n$. Since these functions are smooth, Φ is smooth. $\square$

Corollary. *If two Lie groups are isomorphic as topological groups, then they are isomorphic as Lie groups.* □

Hence, it follows that *if it is possible to introduce on a topological group a smoothness compatible with the topology so that the group should become a Lie group, then this can be done only in one way.*

This means that the forgetful functor

$$\text{GR-DIFF} \to \text{GR-TOP}$$

sends distinct Lie groups to distinct topological groups. We may thus assume that this functor realizes an embedding of the category GR-DIFF in the category GR-TOP. In other words, the category GR-DIFF of Lie groups may be regarded as a subcategory of the category GR-TOP of all topological groups. Then Proposition 5 will mean that the subcategory is complete.

The question now naturally arises as to whether it is possible to characterize the subcategory GR-DIFF within the category GR-TOP by general topological conditions without considering smoothness, i.e. whether it is possible to characterize within the category GR-TOP the topological groups G admitting a Lie group structure.

One necessary condition is obvious: a topological group G admitting a Lie group structure must necessarily be Hausdorff and locally compact. We introduce the following definition to formulate a finer necessary condition:

Definition 3. A topological group G is said to be a group *without small subgroups* if its identity e has a neighbourhood containing no subgroups $H \neq \{e\}$.

It turns out that this property is necessary for a Lie group structure to be introduced in G.

Proposition 6. *Every Lie group G (more precisely, every topological group G_{top} obtained from G by ignoring smoothness) is a group without small subgroups.*

Proof. Introduce a Euclidean metric on a vector space $\mathsf{T}_e(G) = \mathfrak{g}$. Then for a sufficiently small $\delta > 0$ a sphere of radius δ with centre at point 0 is a normal neighbourhood of that point and hence its image under mapping the exp is a normal neighbourhood of the identity in G. Let U be a normal neighbourhood similarly constructed from the

number $\delta/2$. It is clear that for any nonzero vector $A \in \mathfrak{g}$ whose length is less than $\delta/2$ there exists an integer m such that the length of the vector mA is greater than $\delta/2$ and less than δ. This means that for any element $a = \exp A$ of U other than unity there is m such that $a^m = \exp mA$ does not belong to U. Therefore U cannot contain any subgroup $H \neq \{e\}$. $\square$

It should be noted that together with the local compactness condition the absence of small subgroups is already sufficient for us to be able to introduce on a Hausdorff group G a Lie group structure (unique, according to the foregoing).

Theorem (Gleason and Yamabe). *A topological Hausdorff group is a Lie group if and only if it is locally compact and has no small subgroups.*

The proof of the Gleason-Yamabe theorem is too cumbersome for us to present it here.

Another necessary condition for a topological group to be a Lie group is that it should be *locally flat*, i.e. that it should be a topological manifold. The question as to whether this necessary condition is sufficient constitutes the content of what is known as *Hilbert's fifth problem* (as formulated at present). A thorough study of the structure of topological groups with small subgroups showed (Montgomery, Zippin, Iwasawa, Gleason, Yamabe) *that no locally flat group can have small subgroups.* In conjunction with the Gleason-Yamabe theorem this immediately yields a positive solution of Hilbert's problem: *any locally flat group is a Lie group.*

For details see [6] and [8].

Lecture 5

Free associative algebras · Free Lie algebras · The basic lemma · The universal enveloping algebra · The embedding of a Lie algebra into its universal enveloping algebra · Proof of the fact that the algebra $\mathfrak{l}\langle X\rangle$ is free · The Poincaré-Birkhoff-Witt theorem · Tensor products of vector spaces and of algebras · Hopf algebras

To prove statement B of Lecture 4, which is of purely algebraic character, we shall develop the corresponding formalism in a somewhat greater generality and detail than is immediately necessary, since this will allow us to present, without loss of time, a number of interesting and important constructions that are useful in many other questions of Lie algebra theory as well.

Let **A** be an arbitrary category of algebras (over a given field $\mathbb{K}$ to be assumed arbitrary in this lecture). According to the general concept of what a "free object" is (which will be fully clarified only on the basis of the general-categorical notion of a conjugate functor) an algebra $\mathscr{F}$ of **A**, with a subset X chosen in it, is said to be a *free algebra* of the category **A** *with a set of free generators* X if for any algebra $\mathscr{A}$ of **A** every mapping $X \to \mathscr{A}$ is uniquely extended to some homomorphism $\mathscr{F} \to \mathscr{A}$.

For example, a free algebra in the category of associative, commutative and unital algebras is the *algebra of polynomials* $\mathbb{K}[X]$ in unknowns ranging over a set X. Similarly, in the category ALG_0-ASS of associative (but, generally speaking noncommutative) unital algebras a free algebra is the *algebra of polynomials in noncommuting unknowns from* X.

We shall denote that algebra by $\mathbb{K}\langle X\rangle$, and, for a finite set $X = \{x_1, \ldots, x_n\}$, by $\mathbb{K}\langle x_1, \ldots, x_n\rangle$.

For the only case of interest to us, where the set X consists of two elements x, y, every element of the algebra $\mathbb{K}\langle x, y\rangle$ can be uniquely represented as a linear combination with coefficients from $\mathbb{K}$ of expressions of the form

$$x^{p_1}y^{q_1} \ldots x^{p_k}y^{q_k} \tag{1}$$

called *monomials in x and y*. Here $p_1, q_1, \ldots, p_k, q_k$ are arbitrary nonnegative integers which are all, with a possible exception of the "extreme" numbers p_1 and q_k, other than zero. If $p_1 = 0$, then the term x^{p_1} is left out and if $q_k = 0$, then y^{q_k} is. The number $n = p_1 + q_1 + \ldots p_k + q_k$ is called the *degree* of monomial (1).

An *empty monomial* (with $k = 0$) identifiable with the identity 1 of the field $\mathbb{K}$ is allowed. Its degree is zero.

The fact that monomials (1) make up a basis of $\mathbb{K}\langle x, y\rangle$ uniquely defines in $\mathbb{K}\langle x, y\rangle$ the operations of addition and multiplication by numbers in $\mathbb{K}$. As to multiplication, it is sufficient to define it with respect to distributivity only for monomials (1). If monomials $x^{p_1}y^{q_1} \ldots x^{p_k}y^{q_k}$ and $x^{r_1}y^{s_1} \ldots x^{r_l}y^{s_l}$ are such that $q_k \neq 0$ and $r_1 \neq 0$ or on the contrary $q_k = 0$ and $r_1 = 0$, then their product is the monomial

$$x^{p_1}y^{q_1} \ldots x^{p_k}y^{q_k}x^{r_1}y^{s_1} \ldots x^{r_l}y^{s_l} \tag{2}$$

resulting from adjoining the second monomial to the first (when $q_k = 0$ and $r_1 = 0$ the terms y^{q_k} and x^{r_1} are naturally left out). But if of the two exponents q_k and r_1 one and only one is zero, then the monomial obtained from expression (2) (which in that case is not a monomial) is taken to be the product of monomials by replacing $x^{p_k}y^{q_k}x^{r_1}$ by $x^{p_k+r_1}$ for $q_k = 0$ and by replacing $y^{q_k}x^{r_1}y^{s_1}$ by $y^{q_k+s_1}$ for $r_1 = 0$. A direct check shows that this multiplication is associative, as required. Its identity is the empty monomial 1.

If now $\{x, y\} \to \mathcal{A}$ is a mapping of the set $\{x, y\}$ into some associative unital algebra $\mathcal{A}$, then on associating with any monomial (1) an element $a^{p_1}b^{q_1} \ldots a^{p_k}b^{q_k}$ of $\mathcal{A}$, where

a and b are images of the generators x and y in $\mathscr{A}$, and extending this correspondence with respect to linearity to arbitrary polynomials we obtain, as a direct easy check shows, a homomorphism $\mathbb{K}\langle x, y\rangle \to \mathscr{A}$ which sends x and y to a and b, i.e. extends the given mapping $\{x, y\} \to \mathscr{A}$. Since an arbitrary extending homomorphism must send monomial (1) to an element $a^{p_1}b^{q_1} \ldots a^{p_k}b^{q_k}$, no other extending homomorphism can exist. This proves that the *algebra* $\mathbb{K}\langle x, y\rangle$ *is a free algebra of the category* ALG$_0$-ASS *with free generators* x *and* y.

The algebra $\mathbb{K}\langle X\rangle$ with any X can be described similarly. The fact that $\mathbb{K}\langle X\rangle$ is free for any X is proved by obvious, self-evident changes for $X = \{x, y\}$.

Free algebras of the category ALG-LIE (they are called *free Lie algebras*) are significantly more difficult to construct. The simplest way is apparently to consider in the Lie algebra $[\mathbb{K}\langle X\rangle]$ adjoined to a polynomial algebra $\mathbb{K}\langle X\rangle$ a subalgebra $\mathfrak{l}\langle X\rangle$ generated by a set X, i.e. the smallest subalgebra containing that set. Just as in the case $X = \{x, y\}$ (see Lecture 4) the elements of the Lie algebra $\mathfrak{l}\langle X\rangle$ are the *Lie polynomials* in the elements of X, i.e. all possible expressions that can be obtained starting from these elements by the operations of addition, multiplication by numbers and the Lie operation $[a, b] = ab - ba$ (all these elements lie of course in $\mathfrak{l}\langle X\rangle$ and at the same time are a subalgebra of the algebra $[\mathbb{K}\langle X\rangle]$). Unfortunately, there are no simple canonical representations (similar to representation of the elements of $\mathbb{K}\langle X\rangle$ as linear combinations of monomials) for the elements of the algebra $\mathfrak{l}\langle X\rangle$, which significantly complicates the study of $\mathfrak{l}\langle X\rangle$.

As in Lecture 4, ι will denote the embedding $\mathfrak{l}\langle X\rangle \to \mathbb{K}\langle X\rangle$, i.e., more precisely, a mapping transforming a Lie polynomial $u \in \mathfrak{l}\langle X\rangle$ to a polynomial ιu in $\mathbb{K}\langle X\rangle$ obtained upon removing all Lie brackets by the formula $[a, b] = ab - ba$.

Proposition 1. *An algebra* $\mathfrak{l}\langle X\rangle$ *is a free Lie algebra with a set of free generators* X.

The proof of this proposition is very complicated. We begin from afar by proving one lemma relating to any Lie algebras.

Let $\mathfrak{g}$ be a Lie algebra (over a field $\mathbb{K}$) and let

$$X = \{x_i,\ i \in I\} \tag{3}$$

be some basis of it (as a vector space). It is not assumed that $\mathfrak{g}$ is finite-dimensional, therefore the index set I considered *to be well-ordered* is in general infinite. (That there is a basis in a vector space is proved without difficulty using Zorn's lemma, since the set of all subspaces of the vector space that have a basis is easily seen to be inductive, and at the same time any proper subspace having a basis may be included, by adding one vector, in a larger subspace that also has a basis).

Next let $\mathscr{V}_I$ be a vector space whose basis consists of elements z_α, whose indices are all possible *monotonic* (i.e. such that $i_1 \leqslant i_2 \leqslant \ldots \leqslant i_n$) sequences $\alpha = (i_1, i_2, \ldots, i_n)$ of elements of the set I.

For every sequence $\alpha = (i_1, \ldots, i_n)$ we will denote the number n of its terms by $|\alpha|$. We count among monotonic sequences also the *empty sequence* $\varnothing$ for which $|\varnothing| = 0$.

The product of the elements a, b of a Lie algebra $\mathfrak{g}$ will be denoted by $[a, b]$.

Lemma 1. *We can associate any element $a \in \mathfrak{g}$ and any element $v \in \mathscr{V}$ with some element $av \in \mathscr{V}_I$ so that the following conditions hold:*

(a) *the element av is linearly dependent on a and v;*

(b) *for any elements a, $b \in \mathfrak{g}$ and any element $v \in \mathscr{V}_I$*

$$[a, b]\, v = a\,(bv) - b\,(av);$$

(c) *if $\alpha = (i_1, \ldots, i_n)$ and $i < i_1$, then*

$$x_i z_\alpha = z_{i\alpha},$$

where $i\alpha = (i, i_1, \ldots, i_n)$.

Proof. By virtue of condition (a) it suffices to construct elements of the form $x_i z_\alpha$. We do this by induction on $|\alpha|$ and i. To carry out this induction it is convenient to require that the lemma should, in addition, satisfy the following condition:

(d) *if $x_i z_\alpha = \sum c_k z_{\beta_k}$, then $|\beta_k| \leqslant |\alpha| + 1$ for all k.*

For $\alpha = \varnothing$ and any i we set by definition

$$x_i z_\varnothing = z_i.$$

Suppose elements $x_j z_\beta$ have already been constructed for all j and all β with $|\beta| < |\alpha|$ and for $j < i$ when $|\beta| = |\alpha|$. Assuming $\alpha = i_1\beta$, we define an element $x_i z_\alpha$ by the formula

$$x_i z_\alpha = \begin{cases} z_{i\alpha} & \text{if} \quad i \leqslant i_1; \\ x_{i_1}(x_i z_\beta) + [x_i, x_{i_1}] z_\beta & \text{if } i > i_1. \end{cases}$$

By condition (d) and the induction hypothesis this definition is correct. It is clear that for an element $x_i z_\alpha$ thus constructed conditions (c) and (d) hold.

Thus all elements $x_i z_\alpha$ and hence (by linearity) all elements av, $a \in \mathfrak{g}$, $v \in \mathscr{V}_I$ are constructed. It remains to check condition (b). It is clear that it suffices to do it only for $a = x_i$, $b = x_j$, $v = z_\alpha$. Thus we have to prove that for any i, j and any monotonic sequences $\alpha = (i_1, \ldots, i_n)$

$$x_i(x_j z_\alpha) - x_j(x_i z_\alpha) = [x_i, x_j] z_\alpha. \tag{4}$$

With $i = j$ this equation is obviously satisfied. In addition, if it is satisfied for a pair (i, j), then it is satisfied for a pair (j, i) as well. We may assume, therefore, without loss of generality that $i > j$.

We carry out induction on $|\alpha|$. If $\alpha = \varnothing$ (and $i > j$), then by definition

$$x_i(x_j z_\varnothing) = x_j(x_i z_\varnothing) + [x_i, x_j] z_\varnothing.$$

Consequently, when $\alpha = \varnothing$ equation (4) is true.

Assuming now that (4) holds for all α with $|\alpha| < n$, we shall consider a sequence $\alpha = (i_1, \ldots, i_n)$ with $|\alpha| = n$. For the formulas to be symmetric we assume $i_1 = k$ and $\beta = (i_2, \ldots, i_n)$.

If $j \leqslant k$, then by definition

$$x_i(x_j z_\alpha) = x_i z_{j\alpha} = x_j(x_i z_\alpha) + [x_i, x_j] z_\alpha,$$

so that in this case equation (4) is true.

Let $j > k$. By the induction assumption equation (4) is true for $\alpha = \beta$ (and any i and j). Therefore

$$\begin{aligned}[x_i, x_j] z_\alpha &= [x_i, x_j](x_k, z_\beta) \\ &= x_k([x_i, x_j] z_\beta) + [[x_i, x_j], x_k] z_\beta \\ &= x_k(x_i(x_j z_\beta)) - x_k(x_j(x_i z_\beta)) + [[x_i, x_j], x_k] z_\beta,\end{aligned}$$

and hence (4) may be written as follows:

$$x_i\,(x_j\,(x_k z_\beta)) - x_j\,(x_i\,(x_k z_\beta)) + x_k\,(x_j\,(x_i z_\alpha)) \\ - x_k\,(x_i\,(x_j z_\alpha)) = [[x_i,\ x_j],\ x_k]\,z_\beta.$$

We denote this equation by $(i,\ j,\ k)$.

Now notice that equations $(j,\ k,\ i)$ and $(k,\ i,\ j)$ obtained from $(i,\ j,\ k)$ by cyclic permutation of indices may be taken to be proved. Indeed, in rewriting the indices $j \mapsto i$, $k \mapsto j$, $i \mapsto k$ the equation $(j,\ k,\ i)$ becomes $(i,\ j,\ k)$ with $i > j$ and $j < k$ and under these assumptions it is already proved. Similarly, in rewriting the indices $k \mapsto j$, $i \mapsto j$, $j \mapsto k$ the equation $(k,\ i,\ j)$ also becomes (with only all the signs changed) an equation $(i,\ j,\ k)$ with $i > j$ and $j < k$.

On the other hand, by adding $(j,\ k,\ i)$ and $(k,\ i,\ j)$ together we obtain on the left just the left-hand side of $(i,\ j,\ k)$ with an opposite sign. As to the right-hand side of the sum it is

$$([[x_j,\ x_k],\ x_i] + [[x_k,\ x_i],\ x_j])\,z_\beta$$

which, by virtue of the Jacobi identity, equals the right-hand side of $(i,\ j,\ k)$ taken with an opposite sign. Consequently, since $(j,\ k,\ i)$ and $(k,\ i,\ j)$ are true so is $(i,\ j,\ k)$.

This completes the proof of Lemma 1. □

Recall that a vector space $\mathscr{V}$ is said to be *a module over an associative algebra* $\mathscr{A}$ (or simply $\mathscr{A}$-module) if for any element $a \in \mathscr{A}$ and any element $v \in \mathscr{V}$ an element $av \in \mathscr{V}$ is defined which is linearly dependent on a and v and if for any elements $a,\ b \in \mathscr{A}$, $v \in \mathscr{V}$

$$(ab)\,v = a\,(bv). \tag{5}$$

The fact that the element av is linearly dependent on v implies that the mapping $v \mapsto av$ of the space $\mathscr{V}$ into itself is linear. Denoting the mapping by $\theta\,(a)$ we thus obtain some mapping θ of the algebra $\mathscr{V}$ into the algebra End $\mathscr{V}$ of all linear mappings (endomorphisms) of $\mathscr{V}$ into itself. The fact that av is linearly dependent on a implies that θ is linear and relation (5) implies that θ is a homomorphism of algebras. Conversely, an arbitrary homomorphism of algebras $\theta\colon \mathscr{A} \to \operatorname{End} \mathscr{V}$ defines on $\mathscr{V}$ the structure of a module over $\mathscr{A}$ for which $av = \theta\,(a)\,v$.

Similarly a vector space $\mathscr{V}$ is said to be *a module over a Lie algebra* $\mathfrak{g}$ if a certain homomorphism $\theta\colon \mathfrak{g} \to [\operatorname{End} \mathscr{V}]$ of the Lie algebra $\mathfrak{g}$ into the Lie algebra $[\operatorname{End} \mathscr{V}]$ is given. In terms of elements this means that for any element $a \in \mathfrak{g}$ and any element $v \in \mathscr{V}$ an element $av = \theta(a)v$ is defined, which is linearly dependent on a and v, with

$$[a, b] = a(bv) - b(av)$$

for any elements $a, b \in \mathfrak{g}$ and $v \in \mathscr{V}$. Comparing these requirements and conditions (a) and (b) of Lemma 1 we see that the lemma implies that *we may introduce into the vector space* $\mathscr{V}_I$ *the structure of a module over* $\mathfrak{g}$ *such that for any monotonic sequence* $\alpha = (i_1, i_2, \ldots, i_n)$ *and any* $i \leqslant i_1$

$$x_i z_\alpha = z_{i\alpha}.$$

It is in this formulation that this lemma will be used.

Now let $\mathfrak{U}$ be some associative unital algebra and let $\iota\colon \mathfrak{g} \to [\mathfrak{U}]$ be a homomorphism of a Lie algebra $\mathfrak{g}$ into a commutator Lie algebra of $\mathfrak{U}$.

Definition 1. A homomorphism $\iota\colon \mathfrak{g} \to [\mathfrak{U}]$ is said to have the *property of being universal* and $\mathfrak{U}$ (considered together with that homomorphism) to be the *universal enveloping algebra* of a Lie algebra $\mathfrak{g}$ if for any associative unital algebra $\mathscr{A}$ and any homomorphism $\varphi\colon \mathfrak{g} \to [\mathscr{A}]$ there exists a unique homomorphism $\psi\colon \mathfrak{U} \to \mathscr{A}$ for which the diagram

$$\begin{tikzcd} \mathfrak{g} \arrow[r, "\iota"] \arrow[d, "\varphi"'] & \mathfrak{U} \arrow[dl, "\psi"] \\ \mathscr{A} & \end{tikzcd}$$

is commutative.

We shall write $\psi = \mathfrak{U}\varphi$.

Notice that if $\mathscr{A} = \mathfrak{U}$ and $\varphi = \iota$, then $\mathfrak{U}\varphi$ is an identity homomorphism $\mathrm{id}\colon \mathfrak{U} \to \mathfrak{U}$.

For a Lie algebra $\mathfrak{l}\langle X\rangle$ *the algebra* $\mathbb{K}\langle X\rangle$ (relative to the embedding $\iota\colon \mathfrak{l}\langle X\rangle \to [\mathbb{K}\langle X\rangle]$) *is the universal enveloping algebra*. Indeed, let $\varphi\colon \mathfrak{l}\langle X\rangle \to [\mathscr{A}]$ be a homomorphism

of $\mathfrak{l}\langle X\rangle$ into a commutator algebra $[\mathscr{A}]$ of some associative unital algebra $\mathscr{A}$. Since $\mathbb{K}\langle X\rangle$ is free, the mapping $\varphi\,|_X\colon X\to\mathscr{A}$ can be uniquely extended to some homomorphism $\psi\colon \mathbb{K}\langle X\rangle\to\mathscr{A}$. It is only necessary to show that $\psi\circ\iota=\varphi$, i.e. that $\psi\,|_{\mathfrak{l}\langle X\rangle}=\varphi$. But by construction $\psi=\varphi$ on X. In addition, if $\varphi a=\psi a$ and $\varphi b=\psi b$, where $a, b\in\mathfrak{l}\langle X\rangle$, then $\varphi(a+b)=\psi(a+b)$, $\varphi(ka)=\psi(kb)$ (for both mappings φ and ψ are linear) and $\varphi[a, b]=[\varphi a, \varphi b]=\varphi a\cdot\varphi b-\varphi b\cdot\varphi a=\psi a\cdot\psi b-\psi b\cdot\psi a=\psi(ab-ba)=\psi[a, b]$. Therefore $\varphi=\psi$ on all Lie polynomials in X, i.e. on the whole of $\mathfrak{l}\langle X\rangle$. □

If $\iota_1\colon \mathfrak{g}\to[\mathcal{U}_1]$ and $\iota_2\colon \mathfrak{g}\to[\mathcal{U}_2]$ are two homomorphisms having the property of being universal, then homomorphisms $\rho=\mathcal{U}_1\iota_2\colon \mathcal{U}_1\to\mathcal{U}_2$ and $\sigma=\mathcal{U}_2\iota_1\colon \mathcal{U}_2\to\mathcal{U}_1$, arising by virtue of universality of ι_1 and ι_2 respectively, are defined:

$$\begin{tikzcd}
\mathfrak{g} \arrow[r, "\iota_1"] \arrow[d, "\iota_2"'] & \mathcal{U}_1 \arrow[dl, shift left, "\rho"] \\
\mathcal{U}_2 \arrow[ur, shift left, "\sigma"'] &
\end{tikzcd}$$

For the composition $\sigma\circ\rho$ a commutative diagram

$$\begin{tikzcd}
\mathfrak{g} \arrow[r, "\iota_1"] \arrow[d, "\iota_2"'] & \mathcal{U}_1 \arrow[dl, "\sigma\circ\rho"] \\
\mathcal{U}_1 &
\end{tikzcd}$$

shows that $\sigma\circ\rho=\mathcal{U}_1\iota_1$. But, as noticed above, $\mathcal{U}_1\iota_1=\mathrm{id}$, where id is an identity mapping $\mathcal{U}_1\to\mathcal{U}_1$. Therefore $\sigma\circ\rho=\mathrm{id}$. We can similarly show that the composition $\rho\circ\sigma$ is an identity mapping $\mathcal{U}_2\to\mathcal{U}_2$. Consequently, the homomorphisms ρ and σ are reciprocal isomorphisms. This proves that *for any two universal enveloping algebras $\mathcal{U}_1$ and $\mathcal{U}_2$ of a Lie algebra $\mathfrak{g}$ there exists an isomorphism $\rho\colon \mathcal{U}_1\to\mathcal{U}_2$ such that $\rho\circ\iota_1=\iota_2$.*

In this sense a universal enveloping algebra $\mathcal{U}$ of a given Lie algebra is unique.

To prove its existence we again choose in $\mathfrak{g}$ an arbitrary basis (3) and consider the algebra of noncommutative polynomials $\mathbb{K}\langle X\rangle$. The algebra $\mathfrak{g}$ (considered as a vector space) is identified naturally with a subspace $\mathbb{K}_1\langle X\rangle$ of $\mathbb{K}\langle X\rangle$ consisting of homogeneous polynomials of the first degree. Thus for any elements $x, y \in \mathfrak{g}$ three elements (clearly distinct for $x \neq 0$ and $y \neq 0$) will be defined in the algebra $\mathbb{K}\langle X\rangle$: an element $[x, y] \in \mathbb{K}_1\langle X\rangle$, a homogeneous first-degree polynomial, and elements xy and yx, homogeneous second-degree polynomials. Let $\mathcal{Y}$ be an ideal of $\mathbb{K}\langle X\rangle$ generated by all polynomials of the form $xy - yx - [x, y]$ and let $\mathcal{U} = \mathbb{K}\langle X\rangle/\mathcal{Y}$ be the corresponding quotient algebra. Also let $\iota\colon \mathfrak{g} \to \mathcal{U}$ be a restriction to $\mathfrak{g} = \mathbb{K}_1\langle X\rangle$ of the canonical epimorphism $\mathbb{K}\langle X\rangle \to \mathcal{U}$. Then for any elements $x, y \in \mathfrak{g}$ in $\mathcal{U}$

$$\iota[x, y] = \iota(xy - yx) = \iota x\cdot\iota y - \iota y\cdot\iota x = [\iota x, \iota y].$$

The equation shows that ι is a homomorphism of Lie algebras $\mathfrak{g} \to [\mathcal{U}]$.

Now let $\mathcal{A}$ be an associative unital algebra and let $\varphi\colon \mathfrak{g} \to [\mathcal{A}]$ be an arbitrary homomorphism. A restriction of φ to X is uniquely extended to some homomorphism $\bar{\psi}\colon \mathbb{K}\langle X\rangle \to \mathcal{A}$. Both mappings φ and $\bar{\psi}$ are linear and coincide on the basis X of the vector space $\mathfrak{g} = \mathbb{K}_1\langle X\rangle$. Therefore $\varphi = \bar{\psi}$ on $\mathfrak{g}$ and hence for any elements $x, y \in \mathfrak{g}$

$$\begin{aligned}\bar{\psi}(xy - yx - [x, y]) &= \bar{\psi}x\cdot\bar{\psi}y - \bar{\psi}y\cdot\bar{\psi}x - \bar{\psi}[x, y]\\ &= \varphi x\cdot\varphi y - \varphi y\cdot\varphi x - \varphi[x, y]\\ &= [\varphi x, \varphi y] - \varphi[x, y] = 0.\end{aligned}$$

Consequently, $\bar{\psi}(\mathcal{Y}) = 0$ and therefore $\bar{\psi}$ induces some homomorphism $\psi\colon \mathcal{U} \to \mathcal{A}$ which obviously has the property that $\varphi \circ \iota = \psi$. This means that the homomorphism ι has the property of being universal.

This proves that *for any Lie algebra $\mathfrak{g}$ there is a universal enveloping algebra $\mathcal{U}$.*

Remark 1. It is easily seen that the constructed algebra $\mathcal{U}$ is independent of the choice of basis (3) of a Lie algebra $\mathfrak{g}$

and therefore the correspondence $\mathfrak{g} \mapsto \mathcal{U}$ is some functor ALG-LIE $\to$ ALG$_0$-ASS. This functor has the property that for any associative algebra $\mathcal{A}$ the set Hom $(\mathfrak{g}, [\mathcal{A}])$ of all homomorphisms $\mathfrak{g} \to [\mathcal{A}]$ is in a natural bijective correspondence with the set Hom $(\mathcal{U}, \mathcal{A})$ of all homomorphisms $\mathcal{U} \to \mathcal{A}$:

$$\mathrm{Hom}\,(\mathfrak{g}, [\mathcal{A}]) \approx \mathrm{Hom}\,(\mathcal{U}, \mathcal{A}).$$

In terms of category theory this means that the functor $\mathfrak{g} \mapsto \mathcal{U}$ *is conjugate from the left* to the commutator functor $\mathcal{A} \mapsto [\mathcal{A}]$.

As applied to the algebra $\mathfrak{g} = \mathrm{End}\,\mathcal{V}$ the property of being universal for a homomorphism $\iota: \mathfrak{g} \mapsto [\mathcal{U}]$ implies that *any module $\mathcal{V}$ over a Lie algebra $\mathfrak{g}$ has a unique structure of a $\mathcal{U}$-module continuing its structure of a $\mathfrak{g}$-module, i.e. such that*

$$xv = (\iota x)_{\bullet} v$$

for any elements $x \in \mathfrak{g}$ and $v \in \mathcal{V}$. Indeed, the structure of a $\mathfrak{g}$-module on $\mathcal{V}$ is given by the homomorphism $\mathfrak{g} \to [\mathrm{End}\,\mathcal{V}]$ and the structure of a $\mathcal{U}$-module is given by the homomorphism $\mathcal{U} \to [\mathrm{End}\,\mathcal{V}]$. □

By virtue of Lemma 1 this implies that *on the vector space $\mathcal{V}_1$ there exists a $\mathcal{U}$-module structure in which*

(6) $$(\iota x_i)\, z_\alpha = z_{i\alpha}$$

for any monotonic sequence $\alpha = (i_1, \ldots, i_n)$ and any $i \leqslant i_1$. In particular

$$(\iota x_i)\, z_{\varnothing} = z_i.$$

The last formula immediately yields the following proposition:

Proposition 2. *For any Lie algebra $\mathfrak{g}$ the mapping $\iota: \mathfrak{g} \to [\mathcal{U}]$ is injective, so that the algebra $\mathfrak{g}$ can be identified with some subalgebra of a commutator algebra $[\mathcal{U}]$.*

Proof. Let x be an element of a Lie algebra $\mathfrak{g}$ such that $\iota x = 0$ and let $x = \sum c_i x_i$ be an expansion of that element with respect to basis (3). Then

$$\sum c_i z_i = \sum c_i\, (\iota x_i)\, z_{\varnothing} = (\iota \sum c_i x_i)\, z_{\varnothing} = (\iota x)\, z_{\varnothing} = 0 z_{\varnothing} = 0,$$

which is possible (since the elements z_i make up a part of

the basis of the vector space $\mathscr{V}_I$) only when $c_i = 0$ for all i. Consequently $x = 0$. □

Proposition 2 explains the attribute "enveloping" for the algebra $\mathfrak{U}$.

In what follows we shall assume the mapping ι to be an embedding and in particular an element of the form ιx, $x \in \mathfrak{g}$ will be denoted simply by x.

Now Proposition 2 easily yields Proposition 1.

Proof of Proposition 1. Let $\varphi: X \to \mathfrak{g}$ be a mapping of a set X into an arbitrary Lie algebra $\mathfrak{g}$ and let $\iota: \mathfrak{g} \to \mathfrak{U}$ be an embedding of the algebra $\mathfrak{g}$ into its universal enveloping algebra $\mathfrak{U}$. Since $\mathbb{K}\langle X\rangle$ is a free algebra of the category ALG_0-ASS, there exists a homomorphism $\bar{\psi}$: $\mathbb{K}\langle X\rangle \to \mathfrak{U}$ coinciding on X with a composite mapping $\iota \circ \varphi$: $X \to \mathfrak{U}$. This homomorphism transforms every element of $\mathfrak{l}\langle X\rangle$, i.e. every Lie polynomial in elements $x \in X$ into a Lie polynomial in the corresponding elements $(\iota \circ \varphi)\, x$ of a subalgebra $\iota(\mathfrak{g})$ and hence into some element of that subalgebra. This means that $\bar{\psi}(\mathfrak{l}\langle X\rangle) \subset \iota(\mathfrak{g})$. Since by Proposition 2 the mapping $\iota: \mathfrak{g} \to \iota(\mathfrak{g})$ is bijective, it follows that $\bar{\psi}$ induces a mapping ψ: $\mathfrak{l}\langle X\rangle \to \mathfrak{g}$ such that $\iota \circ \psi = \bar{\psi}$ on $\mathfrak{l}\langle X\rangle$. To complete the proof it remains to notice that ψ is obviously a homomorphism of Lie algebras and coincides on X with a given mapping φ. □

Proposition 2 is equivalent to the assertion that elements $x_i = \iota x_i$ of $\mathfrak{U}$ are linearly independent. In this form it allows an important generalization which plays an essential role in the proof of statement B of the preceding lecture (it should also be noticed that in fact we do not need Proposition 1 to prove statement B; we have proved it only because it is of interest in its own right). To formulate this generalization consider for any monotonic sequence $\alpha = (i_1, i_2, \ldots, i_n)$ of the elements of the set I an element

$$x_\alpha = x_{i_1} x_{i_2} \ldots x_{i_n} \tag{7}$$

of $\mathfrak{U}$ (it is assumed for $\alpha = \varnothing$ that $x_\varnothing = 1$). In what follows, for ease of formulations, we shall call elements of the form (7) *special elements* of $\mathfrak{U}$ (with respect to basis (3) of $\mathfrak{g}$).

Proposition 3. *Special elements x_α of a universal enveloping algebra $\mathfrak{U}$ are linearly independent.*

Proof. Formula (6) yields by an obvious induction that

$$x_\alpha z_\varnothing = z_\alpha$$

for any monotonic sequence α. After that it remains to repeat the already familiar argument: if $\sum c_\alpha x_\alpha = 0$, then

$$\sum c_\alpha z_\alpha = \sum c_\alpha x_\alpha z_\varnothing = 0 z_\varnothing = 0,$$

which is possible only if $c_\alpha = 0$ for any α. $\square$

Proposition 3 can be made more precise:

Proposition 4. *Special elements x_α form a basis of an algerba $\mathfrak{U}$ (considered as a vector space).*

Before proving this proposition we make some preliminary remarks.

Of course, elements $\dot{x}_\alpha$ are defined for *any* (not necessarily monotonic) sequences $\alpha = (i_1, \ldots, i_n)$ of elements of the set I (but the word "special" will be used for these elements only if the sequence α is monotonic).

For any sequence $\alpha = (i_1, \ldots, i_n)$ of elements of I we denote by $d(\alpha)$ the number of *disorders* it has, i.e. pairs (k, l), $1 \leqslant k, l \leqslant n$, such that $k < l$ and $i_k > i_l$. The sequence α is monotonic if and only if $d(\alpha) = 0$. In particular $d(\varnothing) = 0$.

An easy induction on $|\alpha|$ and $d(\alpha)$ now shows that *any element of the form x_α is a linear combination of special elements.*

For $d(\alpha) = 0$ this assertion is indeed true. Assuming that it has already been proved for all elements of the form x_β with $|\beta| < |\alpha|$ or with $|\beta| = |\alpha|$ and $d(\beta) < d(\alpha)$ consider an element x_α with $d(\alpha) > 0$. It is clear that the sequence α has a pair of adjacent indices (i, j) that form a disorder, i.e. such that $i > j$. The element x_α can therefore be written as follows:

$$x_\alpha = x_{\alpha'} x_i x_j x_{\alpha''},$$

where α' and α'' are some sequences (possibly empty) of indices. But by definition of a commutator

$$x_i x_j = x_j x_i + [x_i, x_j],$$

and therefore

$$x_\alpha = x_{\alpha'} x_j x_i x_{\alpha''} + x_{\alpha'} [x_i, x_j] x_{\alpha''}.$$

In $\mathfrak{g}$ the element $[x_i, x_j]$ is expanded with respect to basis (3), i.e. we have an equation of the form

$$[x_i, x_j] = c_{k_1} x_{k_1} + c_{k_2} x_{k_2} + \ldots,$$

where only a finite number of coefficients $c_{k_1}, c_{k_2}, \ldots$ are nonzero. Hence

$$x_\alpha = x_{\beta_0} + c_{k_1} x_{\beta_1} + c_{k_2} x_{\beta_2} + \ldots,$$

where

$$x_{\beta_0} = x_{\alpha'} x_j x_i x_{\alpha''} \text{ and } x_{\beta_s} = x_{\alpha'} x_{k_s} x_{\alpha''} \text{ for}$$
$$s = 1, 2, \ldots,$$

Since $d(\beta_0) = d(\alpha) - 1$ and $|\beta_s| = |\alpha| - 1$ for $s > 0$, the elements x_{β_0} and x_{β_s} can be expressed by the induction assumption in terms of special elements. Hence so can the element x_α. $\square$

On the other hand, it immediately follows from the above construction of a universal enveloping algebra $\mathcal{U}$ that $\mathcal{U}$ *is generated* (*as a unital algebra*) *by all elements of* $\mathfrak{g}$, i.e., more precisely, elements of the form ιx, where $x \in \mathfrak{g}$. However, this assertion easily follows directly from Definition 1. Indeed, let $\mathcal{V}$ be a subalgebra of $\mathcal{U}$ generated by all elements of $\mathfrak{g}$ (and the identity 1) and let $j\colon \mathcal{V} \to \mathcal{U}$ be a homomorphism of embedding. Since $\iota\mathfrak{g} \subset \mathcal{V}$, the homomorphism ι induces a homomorphism $\iota'\colon \mathfrak{g} \to [\mathcal{V}]$ (satisfying the relation $j \circ \iota' = \iota$). Let $k = \mathcal{U}\iota'$. Then, as directly follows from the commutative diagram

$$\begin{tikzcd}
& \mathfrak{g} \arrow[r, "\iota"] \arrow[dl, "\iota"'] \arrow[d, "\iota'"] & \mathcal{U} \arrow[dl, "k"] \\
\mathcal{U} & \mathcal{V} \arrow[l, "j"] &
\end{tikzcd}$$

the composition $j \circ k$ is a mapping $\mathcal{U}\iota = \mathrm{id}$. Consequently the homomorphism j is an epimorphism. Hence $\mathcal{V} = \mathcal{U}$. $\square$

Proof of Proposition 4. According to Proposition 3 it is sufficient to prove that any element of $\mathcal{U}$ is a linear combination of special elements. But since elements in $\mathfrak{g}$ generate an algebra $\mathcal{U}$, any element of that algebra is a polynomial in elements x_i of basis (3), i.e. it is a linear combination of monomials of the form x_α (with an arbitrary α). This proves Proposition 4, since, as proved above, every element of the form x_α is a linear combination of special elements.

Proposition 4 is usually referred to as the *Poincaré-Birkhoff-Witt theorem*. However, this name is also given to Propositions 2 and 3.

We shall need Proposition 4 only in application to the algebra $\mathfrak{l}\langle X\rangle$ and its universal enveloping algebra $\mathbb{K}\langle X\rangle$ (so that strictly speaking we could have done without the notion of enveloping algebra; but no significant simplifications would have resulted).

The next step in the proof of statement B is to characterize in a different, more efficient way the elements of $\mathfrak{l}\langle X\rangle$. To do this we shall need one general construction.

Let $\mathcal{A}$ and $\mathcal{B}$ be two vector spaces and let $\{x_i\}$ and $\{y_j\}$ be some bases of them. Consider all possible formal products of the form x_iy_j and a vector space $\mathcal{C}$ whose basis they are. Every element of $\mathcal{C}$ is a formal linear combination of the form

$$\sum k_{ij}x_iy_j, \qquad k_{ij} \in \mathbb{K},$$

with only a finite number of coefficients k_{ij} other than zero. Compare $\mathcal{C}$ and $\mathcal{C}'$ whose elements are formal sums of the form

$$\sum a_jy_j, \tag{8}$$

where $a_j \in \mathcal{A}$, and in which linear operations are defined in the obvious way ($\mathcal{C}'$ is a direct sum of vector spaces isomorphic to $\mathcal{A}$ whose number equals that of the elements of $\{y_j\}$). Notice that $\mathcal{C}'$ *is independent* of the choice of the basis $\{x_i\}$ (that basis is not involved in its construction). If $a_j = \sum k_{ij}x_i$ are expansions of elements a_j with respect to $\{x_i\}$, then we associate the element $\sum k_{ij}x_iy_j$ of $\mathcal{C}$ with element (8) of $\mathcal{C}'$. This obviously establishes an isomorphism of $\mathcal{C}'$ onto $\mathcal{C}$. On identifying by means of that isomorphism $\mathcal{C}'$ and $\mathcal{C}$ we

thus see that $\mathscr{C}$ is also independent of the choice of the basis $\{x_i\}$. In addition, the identification makes meaningful (and valid) the equation

$$\sum k_{ij}x_iy_j = \sum (\sum k_{ij}x_i)\, y_j.$$

Similarly $\mathscr{C}$ is identified with a vector space $\mathscr{C}''$ whose elements are of the form

$$\sum x_ib_i,$$

where $b_i \in \mathscr{B}$. This proves that $\mathscr{C}$ is independent of the choice of basis $\{y_j\}$ and at the same time makes meaningful the equation

$$\sum k_{ij}x_iy_j = \sum x_i\,(\sum k_{ij}y_j).$$

We thus see that $\mathscr{C}$ is independent (by virtue of the above identifications) of the choice of bases in $\mathscr{A}$ and $\mathscr{B}$, i.e. it is defined by $\mathscr{A}$ and $\mathscr{B}$ only. It is called a *tensor product* of vector spaces $\mathscr{A}$ and $\mathscr{B}$ and is denoted by $\mathscr{A} \otimes \mathscr{B}$.

Remark 1. The elements x_iy_i of $\mathscr{A} \otimes \mathscr{B}$ are usually denoted by $x_i \otimes y_j$ and accordingly the element $\sum k_{ij}x_iy_j$ is written as $\sum k_{ij}x_i \otimes y_j$. More generally, for any two elements $a = \sum k_ix_i$ and $b = \sum l_jy_j$ we denote an element $\sum k_il_jx_i \otimes y_j$ by $a \otimes b$. It is clear that

$$(a_1 + a_2) \otimes b = a_1 \otimes b + a_2 \otimes b,$$
$$a \otimes (b_1 + b_2) = a \otimes b_1 + a \otimes b_2,$$

and

$$k\,(a + b) = (ka) \otimes b_1 = a \otimes (kb)$$

for any elements a, a_1, $a_2 \in \mathscr{A}$, b, b_1, $b_2 \in \mathscr{B}$ and $k \in \mathbb{K}$. Conversely, it is not hard to see that the vector space generated by the symbols $a \otimes b$ subject to these relations is naturally isomorphic to the vector space $\mathscr{A} \otimes \mathscr{B}$. Thus we obtain an invariant construction (using no bases) of $\mathscr{A} \otimes \mathscr{B}$. We shall not need that construction and therefore we are not going to dwell on it in greater detail.

Remark 2. One can obtain another invariant characterization of the vector space $\mathscr{A} \otimes \mathscr{B}$ (at least for the case where $\mathscr{A}$ and $\mathscr{B}$ are both finite-dimensional vector spaces) if one

considers a vector space $\mathscr{D}$ of mixed bilinear functionals x, $y \longmapsto B(x, y)$ (see II, 5), with the first independent variable ranging over $\mathscr{A}$ and the second over $\mathscr{B}$. It turns out that $\mathscr{A} \otimes \mathscr{B}$ is conjugate to $\mathscr{D}$, the corresponding pairing being uniquely defined by the relation $\langle a \otimes b, \boldsymbol{B} \rangle = \boldsymbol{B}(a, b)$. This remark will not be used either.

In the case where $\mathscr{A}$ and $\mathscr{B}$ are algebras, multiplication is defined in $\mathscr{A} \otimes \mathscr{B}$ such that

$$(a \otimes b)\,(x \otimes y) = (ax) \otimes (by)$$

for any $a, x \in \mathscr{A}$, $b, y \in \mathscr{B}$. Under that multiplication $\mathscr{A} \otimes \mathscr{B}$ is an algebra. This is called a *tensor product* of algebras $\mathscr{A}$, $\mathscr{B}$ and denoted by the same symbol $\mathscr{A} \otimes \mathscr{B}$.

If $\mathscr{A}$ and $\mathscr{B}$ are associative and unital algebras, then so is $\mathscr{A} \otimes \mathscr{B}$. (Notice that for a Lie algebra a similar statement is false.) The identity of $\mathscr{A} \otimes \mathscr{B}$ is obviously the element $1 \otimes 1$.

In our simplified notation (with $\otimes$ omitted) multiplication in $\mathscr{A} \otimes \mathscr{B}$ is given as follows:

$$\left(\sum k_{ij} x_i y_j\right) \left(\sum l_{pq} x_p y_q\right) = \sum k_{ij} l_{pq} \,(x_i x_p)\,(y_j y_q).$$

In the only case of interest to us where $\mathscr{A} = \mathbb{K}\langle X \rangle$ and $\mathscr{B} = \mathbb{K}\langle Y \rangle$, the algebra $\mathscr{A} \otimes \mathscr{B}$ is nothing but the algebra of polynomials in the generators of X and Y subject to the requirement that every generator in X commutates with every generator in Y. We shall denote that algebra by $\mathbb{K}\langle X, Y \rangle$. Thus

$$\mathbb{K}\langle X, Y \rangle = \mathbb{K}\langle X \rangle \otimes \mathbb{K}(Y)$$

for any X and Y.

Multiplication in an arbitrary algebra $\mathscr{A}$ is nothing but some linear mapping

$$\mu\colon \mathscr{A} \otimes \mathscr{A} \to \mathscr{A}$$

(the image of an element $a \otimes b \in \mathscr{A} \otimes \mathscr{B}$ under that mapping is a product ab). By the category-theoretic duality (consisting in inverting all the arrows) the dual object is an arbitrary linear mapping

$$\delta\colon \mathscr{A} \to \mathscr{A} \otimes \mathscr{A}. \tag{9}$$

The vector space $\mathcal{A}$ for which some mapping of the form (9) is given is called a *coalgebra* and mapping (9) is a *comultiplication* (the term *diagonal mapping* is also used).

Definition 2. An associative unital algebra $\mathcal{A}$ is said to be a *Hopf algebra* if it is at the same time a coalgebra (i.e. if a comultiplication is given for it), with

(a) comultiplication (9) being a homomorphism of unital algebras;

(b) a linear subspace $\mathcal{A}^*$ given in $\mathcal{A}$ such that $\mathcal{A} = \mathbb{K}\,1 \otimes \mathcal{A}^*$ and for any element $x \in \mathcal{A}^*$

$$\delta x = 1 \otimes x + x \otimes 1 + \sum x_i \otimes y_i, \tag{10}$$

where $x_i y_i \in \mathcal{A}^*$. If

$$\delta x = 1 \otimes x + x \otimes 1,$$

then the element $x \in \mathcal{A}^*$ is said to be *primitive*.

Notice that according to (a) $\delta 1 = 1 \otimes 1$.

In terms of the general theory of coalgebras condition (b) means that an element $1 \in \mathcal{A}$ is the *coidentity* of comultiplication δ.

The mappings $x \mapsto x \otimes 1$ and $x \mapsto 1 \otimes x$ are monomorphisms of $\mathcal{A}$ into $\mathcal{A} \otimes \mathcal{A}$. We shall denote an element $x \otimes 1$ by x' and $1 \otimes x$ by x''. In this notation formula (10) becomes

$$\delta x = x' + x'' + \sum x_i' y_i'', \tag{11}$$

where x_i, $y_i \in \mathcal{A}^*$ and the primitivity condition becomes

$$\delta x = x' + x''.$$

According to the above remark, if $\mathcal{A} = \mathbb{K}\langle X \rangle$, serving as the algebra $\mathcal{A} \otimes \mathcal{A}$ is the algebra $\mathbb{K}\langle X', X'' \rangle$, where X' and X'' are two disjoint specimens of a set X. If in particular $\mathcal{A} = \mathbb{K}\langle x, y \rangle$ (it is in fact this case that is of interest to us), then $\mathcal{A} \otimes \mathcal{A} = \mathbb{K}\langle x', y'; x'', y'' \rangle$, where x' and y' commute with x'' and y''.

We introduce a comultiplication into the algebra $\mathbb{K}\langle X \rangle$, requiring that all generators $x \in X$ should be primitive, i.e. that for any element $x \in X$ there should be a formula

$$\delta x = x' + x''.$$

Since $\mathbb{K}\langle X\rangle$ is a free algebra, that condition uniquely defines a comultiplication

(12) $$\delta\colon \mathbb{K}\langle X\rangle \to \mathbb{K}\langle X', X''\rangle$$

which is a homomorphism of algebras, i.e. satisfies condition (a) in the definition of a Hopf algebra.

As to condition (b), as the linear subspace $\mathcal{A}^*$ we take the subalgebra $\mathbb{K}\langle X\rangle^*$ of the algebra $\mathbb{K}\langle X\rangle$ which consists of all *polynomials without a free term* (the polynomials being linear combinations of monomials $\neq 1$) or, obviously equivalently, which is the span of all special (relative to some basis of the algebra $\mathfrak{l}\langle X\rangle$) elements x_α corresponding to nonempty monotonic sequences α. It is clear that then condition (b) (in the form (11)) holds. Thus *we have given in* $\mathbb{K}\langle X\rangle$ *the structure of a Hopf algebra.*

That structure can be introduced using general considerations in a universal enveloping algebra $\mathcal{U}$ of an arbitrary Lie algebra $\mathfrak{g}$ as well as in $\mathbb{K}\langle X\rangle$. Indeed, since in $\mathcal{U} \otimes \mathcal{U}$ elements with a different number of primes commute the mapping

$$x \mapsto x' + x'', \quad x \in \mathfrak{g},$$

is a homomorphism of $\mathfrak{g}$ into a commutator algebra $[\mathcal{U} \otimes \mathcal{U}]$. It is therefore extended to some homomorphism of algebras

(13) $$\delta\colon \mathcal{U} \to \mathcal{U} \otimes \mathcal{U}.$$

It is now clear that if $\mathcal{U}^*$ is taken to be the subspace of the algebra $\mathcal{U}$, which consists of linear combinations of products of elements from $\mathfrak{g}$, then $\mathcal{U}$ is a Hopf algebra with comultiplication δ. Thus a *universal enveloping algebra* $\mathcal{U}$ *of an arbitrary Lie algebra* $\mathfrak{g}$ *is naturally a Hopf algebra.*

Notice that if $\mathcal{U} = \mathbb{K}\langle X\rangle$, comultiplication (13) coincides with comultiplication (12), since both comultiplications act equally on generators from X.

Lecture 6

The Friedrichs theorem • The proof of Statement **B** *of lecture 4 • The Dynkin theorem • The linear part of a Campbell-Hausdorff series • The convergence of a Campbell-Hausdorff series • Lie group algebras • The equivalence of the categories of local Lie groups and of Lie group algebras • Isomorphism of the categories of Lie group algebras and of Lie algebras • Lie's third theorem*

According to the construction presented at the end of the preceding lecture *all elements of a Lie algebra* $\mathfrak{g}$ *are primitive elements of a universal enveloping algebra* $\mathcal{U}$. The converse turns out to be true as well:

Proposition 1. *For any Lie algebra* $\mathfrak{g}$ *all primitive elements of an enveloping Hopf algebra* $\mathcal{U}$ *are exhausted by elements from* $\mathfrak{g}$.

Proof. Suppose as in the preceding lecture that $X = \{x_i, i \in I\}$ is a basis of a Lie algebra $\mathfrak{g}$ and that $\{x_\alpha\}$ is a basis of an enveloping algebra $\mathcal{U}$ which consists of special (relative to X) elements x_α. Calculate the image δx_α of a special element x_α under comultiplication

$$\delta: \mathcal{U} \to \mathcal{U} \otimes \mathcal{U}.$$

If $\alpha = \varnothing$, i.e. $x_\alpha = 1$, there is no problem: $\delta 1 = 1$. Nor is there any problem if $|\alpha| = 1$, i.e. when α consists of a single element $i \in I$, since an element x_i, being an element of $\mathfrak{g}$, is primitive and therefore $\delta x_i = x_i' + x_i''$. Thus it is only necessary to consider the case of $|\alpha| > 1$.

In general, a sequence α may have equal elements. Let $j_1 < j_2 < \ldots < j_m$ be all nonrecurrent elements of that sequence and let $k_s = k_s(\alpha)$ be the number of elements in α

equal to j_s, $s = 1, \ldots, m$. Thus $k_s \geqslant 1$, $k_1 + \ldots + k_s = |\alpha|$ and

$$x_\alpha = x_{j_1}^{k_1} \ldots x_{j_m}^{k_m}.$$

Since $\delta x_j = x'_j + x''_j$, we have

$$\delta x_\alpha = (x'_{j_1} + x''_{j_1})^{k_1} \ldots (x'_{j_m} + x''_{j_m})^{k_m}.$$

Removing the brackets in this polynomial and writing out only the terms that either contain no differently primed elements or are linear in elements of the form x''_i, we obtain for δx_α (taking into account the commutation of elements with a different number of primes) expressions of the form

$$\begin{aligned}\delta x_\alpha = {} & x'^{k_1}_{j_1} \ldots x'^{k_m}_{j_m} + x''^{k_1}_{j_1} \ldots x''^{k_m}_{j_m} \\ & + k_1 x'^{k_1-1}_{j_1} x'^{k_2}_{j_2} \ldots x'^{k_m}_{j_m} \cdot x''_{j_1} \\ & + k_2 x'^{k_1}_{j_1} x'^{k_2-1}_{j_2} \ldots x'^{k_m}_{j_m} \cdot x''_{j_2} \\ & \cdots\cdots\cdots\cdots\cdots\cdots \\ & + k_m x'^{k_1}_{j_1} x'^{k_2}_{j_2} \ldots x'^{k_m-1}_{j_m} \cdot x''_{j_m} + \ldots,\end{aligned}$$

where in view of the condition $|\alpha| > 1$ no term can cancel one another. Setting

$$x_{\alpha_1} = x_{j_1}^{k_1-1} x_{j_2}^{k_2} \ldots x_{j_m}^{k_m}, \ \ldots, \ x_{\alpha_m} = x_{j_1}^{k_1} x_{j_2}^{k_2} \ldots x_{j_m}^{k_m-1}$$

we can write that formula in the following compact form:

(1) $$\delta x_\alpha = x'_\alpha + x''_\alpha + k_1(\alpha) x'_{\alpha_1} x''_{j_1} + \ldots + k_m(\alpha) x'_{\alpha_m} x''_{j_m} + \ldots, \quad |\alpha| > 1.$$

Consider now an element

$$a = \sum_{\alpha \neq \varnothing} c_\alpha x_\alpha$$

of a vector space $\mathfrak{U}^*$.

Set $a = a_1 + a_2$, where

$$a_1 = \sum_{|\alpha|=1} c_\alpha x_\alpha \quad \text{and} \quad a_2 = \sum_{|\alpha|>1} c_\alpha x_\alpha.$$

The element a_1 is in $\mathfrak{g}$ and therefore it is primitive. Hence a is primitive if and only if so is a_2. In particular, if $a_2 = 0$, then a is primitive.

Let $a_2 \neq 0$ and let $j_1 < \ldots < j_m$ be all distinct elements of all possible sequences α such that x_α appears in a_2 with a nonzero coefficient c_α. For all such x formula (1) remains valid, assuming that $k_s(\alpha) = 0$ and $x_{\alpha_s} = 1$ for each subscript $s = 1, \ldots, m$, such that the element j_s does not appear in α. Therefore

$$\delta a_2 = \sum_{|\alpha|>1} c_\alpha (x'_\alpha + x''_\alpha + k_1(\alpha) x'_{\alpha_1} x''_{j_1} + \ldots + k_m(\alpha) x'_{\alpha_m} x''_{j_m} + \ldots)$$

$$= a'_2 + a''_2 + \Big(\sum_{|\alpha|>1} k_1(\alpha) c_\alpha x'_{\alpha_1}\Big) x''_{j_1} + \ldots + \Big(\sum_{|\alpha|>1} k_m(\alpha) c_\alpha x'_{\alpha_m}\Big) x''_{j_m} + \ldots$$

and hence if a_2 is primitive, then for any $s = 1, \ldots, m$ in $\mathcal{U}$ we have

$$\sum_{|\alpha|>1} k_s(\alpha) c_\alpha x_{\alpha_s} = 0.$$

In this equation the terms corresponding to different sequences α do not cancel since $x_{\alpha_s} = x_{\beta_s}$ only for $\alpha_s = \beta_s$ while if $\alpha_s = \beta_s$ and $k_s(\alpha) \neq 0$, $k_s(\beta) \neq 0$, then $\alpha = \beta$. Hence if a_2 is primitive, then $k_s(\alpha) c_\alpha = 0$ for any sequence α (involved in the expansion of the element a_2) and any s, i.e. (since it is assumed that $c_\alpha \neq 0$) $k_s(\alpha) = 0$. Therefore $|\alpha| = 0$, which contradicts the condition $|\alpha| > 1$.

Consequently, every element $a_2 \neq 0$ is obviously imprimitive. Hence so is a.

This proves that $a \in \mathcal{U}^*$ is primitive if and only if $a_2 = 0$, i.e. if $a = a_1$ and hence $a \in \mathfrak{g}$.

This completes the proof of Proposition 1. □

Corollary (Friedrichs' theorem). *An element of the algebra of polynomials* $\mathbb{K}\langle X\rangle$ *is a Lie polynomial over* X *(i.e. more precisely is of the form* ιa*, where* $a \in \mathfrak{l}\langle X\rangle$*) if and only if that element is primitive.* □

We are now in a position to prove statement B of Lecture 4. Recall that that statement refers to polynomials

$$(2)\qquad z_n(x, y) = \sum_{k=1}^{n} \frac{(-1)^{k-1}}{k} \sum \frac{x^{p_1}y^{q_1} \dots x^{p_k}y^{q_k}}{p_1!\, q_1! \dots p_k!\, q_k!}$$

of the algebra $\mathbb{K}\langle x, y\rangle$ where the internal sum is summed up over all sets of integral nonnegative numbers $p_1, \dots, p_k, q_1, \dots, q_k$ such that $p_1 + \dots + p_k + q_1 + \dots q_k = n$ and $p_i + q_i > 0$ for any $i = 1, \dots, n$ (the field $\mathbb{K}$ will now be assumed to be a field of characteristic 0). These polynomials are homogeneous, degree n components of a formal series $\ln(e^x e^y)$ in two noncommuting variables x and y that results from substituting the product

$$e^x e^y = \sum_{p,\, q=0}^{\infty} \frac{x^p y^q}{p!\, q!}$$

of series

$$e^x = \sum_{p=0}^{\infty} \frac{x^p}{p!} \quad \text{and} \quad e^y = \sum_{q=0}^{\infty} \frac{y^q}{q!}$$

for z in the formal series

$$\ln z = \sum_{k=1}^{\infty} \frac{(-1)^{k-1}}{k} (z - 1)^k.$$

Statement B says that *every polynomial $z_n(x, y)$ is in the algebra $\mathfrak{l}\langle x, y\rangle$*, i.e. by the Friedrichs theorem is a primitive element of the Hopf algebra $\mathbb{K}\langle x, y\rangle$ (satisfies the relation $\delta z_n(x, y) = z_n(x', y') + z_n(x'', y'')$).

Conceptually the most natural way of proving that statement is to extend the algebra $\mathbb{K}\langle x, y\rangle$ to the algebra $\mathbb{K}\langle\langle x, y\rangle\rangle$ of formal series in noncommuting variables x, y and to repeat for that algebra everything we have done in the preceding lecture, i.e. the introduction of a subalgebra $\mathfrak{l}\langle\langle x, y\rangle\rangle$ of the commutator Lie algebra $[\mathbb{K}\langle\langle x, y\rangle\rangle]$ generated by the elements x, y (the latter algebra consists of series, all of whose homogeneous components are Lie polynomials in $\mathfrak{l}\langle x, y\rangle$) and the proof that the series in $\mathfrak{l}\langle\langle x, y\rangle\rangle$ are

exactly the primitive elements of the algebra with respect to a multiplication δ such that $\delta x = x' + x''$ and $\delta y = y' + y''$. As soon as this is done, statement B (equivalent to the statement that the series $\ln(e^x e^y)$ is in the algebra $\mathfrak{l}\langle\langle x, y\rangle\rangle$, i.e. is a primitive element of $\mathbb{K}\langle\langle x, y\rangle\rangle$) is proved by an obvious calculation:

$$
\begin{aligned}
(3) \qquad \delta \ln(e^x e^y) &= \ln(e^{\delta x} e^{\delta y}) = \ln(e^{x'+x''} e^{y'+y''}) \\
&= \ln(e^{x'} e^{x''} e^{y'} e^{y''}) = \ln(e^{x'} e^{y'} e^{x''} e^{y''}) \\
&= \ln(e^{x'} e^{y'}) + \ln(e^{x''} e^{y''}) \\
&= \ln(e^x e^y)' + \ln(e^x e^y)''.
\end{aligned}
$$

(This calculation uses an obvious fact that if elements ξ and η commute, then $e^{\xi+\eta} = e^{\xi} e^{\eta}$ and $\ln(\xi\eta) = \ln \xi + \ln \eta$.)

But in fact there is no need in going over to $\mathbb{K}\langle\langle x, y\rangle\rangle$. Indeed, if we wish to prove the formula $\delta z_n(x, y) = z_n(x', y') + z_n(x'', y'')$ we can repeat manipulation (3), considering not the formal series but only some sufficiently long (depending on n) parts of them and keeping watch on terms of degree $\leqslant n$. It is clear that the entire whole manipulation (which is now realized within $\mathbb{K}\langle\langle x, y\rangle\rangle$) is fully preserved. Thus statement B may at last be considered to be proved.

The above proof of statement B yields no explicit formula for Lie polynomials $\mathfrak{z}_n(x, y)$ whose existence it asserts. We therefore supplement it now by deriving an explicit formula of that kind.

Suppose, as in the preceding lecture, that $\mathbb{K}^*\langle x, y\rangle$ is a subalgebra of $\mathbb{K}\langle x, y\rangle$ consisting of all polynomials without a free term. We define a mapping

$$\sigma\colon \mathbb{K}^*(x, y) \to \mathfrak{l}\langle x, y\rangle$$

in terms of the following conditions;

(a) the mapping σ is linear;

(b) $\sigma x = x$ and $\sigma y = y$;

(c) for any monomial $a \neq 1$

$$\sigma(ax) = [\sigma a, x], \qquad \sigma(ay) = [\sigma a, y].$$

It is clear that these conditions uniquely define a mapping σ.

Definition 1. Elements of the algebra $\mathfrak{l}\langle x, y\rangle$ that are of the form σa where a is a monomial, are called *Lie monomials.*

According to the definition:

(i) elements x and y are Lie monomials;

(ii) if u is a Lie monomial, then so are $[u, x]$ and $[u, y]$.

It is clear that the span of all Lie monomials coincides with the image $\operatorname{Im}\sigma = \sigma(\mathbb{K}^*\langle x, y\rangle)$ of the mapping σ.

In explicit form a Lie monomial σa corresponding to a monomial $a = x^{p_1}y^{q_1} \ldots x^{p_k}y^{q_k}$ is defined as follows

$$\sigma a = [\ldots [\underbrace{x, x], x], \ldots x]}_{p_1 \text{ times}}, \underbrace{y], \ldots, y]}_{q_1 \text{ times}}, \tag{4}$$

$$\ldots, \underbrace{x], \ldots, x]}_{p_k \text{ times}}, \underbrace{y], \ldots, y]}_{q_k \text{ times}}.$$

In particular we see that $\sigma a = 0$ if either $p_1 > 1$ or $p_1 = 0$ and $q_1 > 1$ (recall that according to our definition of a monomial all exponents $p_1, q_1, \ldots, p_k, q_k$ are positive, with the possible exception of p_1 and q_k.)

It follows immediately from (4) that *for any Lie monomial $u = \sigma a$ the polynomial ιu is a homogeneous element of* $\mathbb{K}\langle x, y\rangle$, i.e. a linear combination of monomials of the same degree $n \geqslant 1$. That degree (equal obviously to that of the monomial a) will be called the degree of the Lie monomial u.

Lemma 1. *For any Lie monomials u and v the element* $[u, v]$ *belongs to the vector space* $\operatorname{Im}\sigma$.

Proof. We proceed by induction on degree n of the element v. If $n = 1$, i.e. if $v = x$ or $v = y$, then $[u, v]$ is by definition a Lie monomial and is therefore in $\operatorname{Im}\sigma$. Let $n > 1$. Then $v = [w, x]$ or $v = [w, y]$ where w is a Lie monomial of degree $n - 1$. Assume for definiteness that $v = [w, x]$ (the case $v = [w, y]$ is quite similar). Then $[u, v] = [u, [w, x]]$ and therefore by the Jacobi identity

$$[u, v] = [[u, w], x] - [[u, x], w].$$

But under the induction hypothesis $[u, w]$ is in $\operatorname{Im}\sigma$ and so is $[[u, w], x]$, i.e. it is a linear combination of Lie monomials. The element $[[u, x], w]$ is also a linear combination of Lie monomials. Therefore $[u, v] \in \operatorname{Im}\sigma$. □

Corollary. *Any element of* $\mathfrak{l}\langle x, y\rangle$ *is a linear combination of Lie monomials. In other words*

$$\operatorname{Im} \sigma = \mathfrak{l}\langle x, y\rangle.$$

Proof. It follows immediately from Lemma 1 that the vector space $\operatorname{Im} \sigma$ is a subalgebra of $\mathfrak{l}\langle x, y\rangle$. Since $x, y \in \operatorname{Im} \sigma$ and $\mathfrak{l}\langle x, y\rangle$ is generated by elements x and y, that vector space must coincide with $\mathfrak{l}\langle x, y\rangle$. □

We now define some *antihomomorphism* of $\mathbb{K}\langle x,y\rangle$ into the algebra $\operatorname{End}_{\text{lin}}(\mathfrak{l}\langle x, y\rangle)$ of linear mappings of $\mathfrak{l}\langle x, y\rangle$ into itself, i.e. a linear mapping

$$\theta\colon \mathbb{K}\langle x, y\rangle \to \operatorname{End}_{\text{lin}}(\mathfrak{l}\langle x, y\rangle)$$

that satisfies the relation $\theta(ab) = \theta(b)\circ\theta(a)$ for any elements $a, b \in \mathbb{K}\langle x, y\rangle$. Since $\mathbb{K}\langle x, y\rangle$ is generated by the elements x and y, such an antihomomorphism is uniquely defined by its values θx and θy on those elements, and since the generators x and y are free generators, the mappings θx and θy can be chosen quite arbitrarily. We define them as follows:

$$(\theta x)\, v = [v, x], \quad (\theta y)\, v = [v, y],$$

where v is an arbitrary element of $\mathfrak{l}\langle x, y\rangle$.

Thus by that definition if $u = x$ or $u = y$, then the mapping $\theta(u)\colon \mathfrak{l}\langle x, y\rangle \to \mathfrak{l}\langle x, y\rangle$ is an internal differentiation $\operatorname{ad}(-u) = -\operatorname{ad} u$ of $\mathfrak{l}\langle x, y\rangle$ (see Lecture 3). It turns out that the equation $\theta u = -\operatorname{ad} u$ (or more exactly $\theta(\iota u) = -\operatorname{ad} u$) is true for every element u of $\mathfrak{l}\langle x, y\rangle$.

Lemma 2. *For any elements* $u, v \in \mathfrak{l}\langle x, y\rangle$ *we have*

$$(\bar{\theta} u)\, v = [v, u] \tag{5}$$

where $\bar{\theta} = \theta \circ \iota$.

Proof. By the corollary to Lemma 1 it suffices to prove equation (5) only for the case where u is a Lie monomial. We proceed by induction on degree n of the element u. If $n = 1$, then $u = x$ or $u = y$ and (5) holds by definition. Let $n > 1$. Then $u = [w, x]$ or $u = [w, y]$ where w is a Lie monomial of degree $n - 1$. Suppose for definiteness that $u = [w, x]$. Since

$$\bar{\theta}\,(w, x) = \theta\,(bx) - \theta\,(xb) = \theta x \cdot \theta b - \theta b \cdot \theta x,$$

where $b = \iota w$, according to the induction hypothesis and the Jacobi identity, we have

$$\begin{aligned}(\bar\theta u)\, v &= (\bar\theta\, [w, x])\, v = (\theta x)\, (\theta b)\, v - (\theta b)\, (\theta x)\, v \\ &= (\bar\theta x)\, (\bar\theta w)\, v - (\bar\theta w)\, (\bar\theta x)\, v \\ &= (\bar\theta x)\, [v, w] - (\bar\theta w)\, [v, x] = [[v, w], x] - [[v, x], w] \\ &= [v, [w, x]] = [v, u]. \ \square\end{aligned}$$

Lemma 3. *For any elements* $a, b \in \mathbb{K}^* \langle x, y\rangle$

$$\sigma\, (ab) = (\theta b)\, (\sigma a). \tag{6}$$

Proof. We may assume without loss of generality that b is a monomial. We proceed by induction on its degree n. If $n = 1$, i.e. if $b = x$ or $b = y$, then (6) follows immediately from the definitions. Let $n > 1$. Then $b = cx$ or $b = cy$, where c is a monomial of degree $n - 1$. Suppose for definiteness that $b = cx$. Since

$$\sigma\, (ab) = \sigma\, (acx) = [\sigma\, (ac), x] = (\theta x)\, (\sigma\, (ac)),$$

according to the induction hypothesis, we have

$$\sigma\, (ab) = (\theta x)\, (\theta c)\, (\sigma a) = \theta\, (cx)\, (\sigma a) = (\theta b)\, (\sigma a). \ \square$$

Lemma 4. *A restriction* $\bar\sigma = \sigma \circ \iota$ *of the mapping* σ *to* $\mathfrak{L} \langle x, y\rangle \subset \mathbb{K}^* \langle x, y\rangle$ *is a differentiation of* $\mathfrak{L} \langle x, y\rangle$, *i.e. for any elements* $u, v \in \mathfrak{L} \langle x, y\rangle$

$$\bar\sigma\, [u, v] = [\bar\sigma u, v] + [u, \bar\sigma v].$$

Proof. Let $\iota u = a$ and $\iota v = b$. Then in view of Lemmas 3 and 2

$$\begin{aligned}\bar\sigma\, [u, v] &= \sigma\, (ab) - \sigma\, (ba) = (\theta b)\, (\sigma a) - (\theta a)\, (\sigma b) \\ &= [\sigma a, b] - [\sigma b, a] = [\sigma a, b] + [a, \sigma b] \\ &= [\bar\sigma u, v] + [u, \bar\sigma v]. \ \square\end{aligned}$$

Now we are in a position to prove our main proposition.

Proposition 2 (Dynkin's theorem). *A homogeneous polynomial* $a \in \mathbb{K} \langle x, y\rangle$ *of degree* $n \geqslant 1$ *is in* $\mathfrak{L} \langle x, y\rangle$ (*i.e. is of the form* ιu, *where* $u \in \mathfrak{L} \langle x, y\rangle$) *if and only if*

$$\iota\, (\sigma a) = na. \tag{7}$$

Proof. If (7) holds, then

$$a = \iota\left(\frac{\sigma a}{n}\right), \quad \text{where } \frac{\sigma a}{n} \in \mathfrak{L}\langle x, y\rangle.$$

Conversely, let $a = \iota u$, where $u \in \mathfrak{L}\langle x, y\rangle$. We may assume without loss of generality that u is a Lie monomial. We proceed by induction on degree n of u. If $n = 1$, then $u = x$ or $u = y$ and (7) holds. Let $n > 1$ and suppose for definiteness that $u = [v, x]$ where v is a Lie monomial of degree $n - 1$. Then according to Lemma 4 and the induction hypothesis

$$\begin{aligned}
\iota(\sigma a) &= \iota(\bar{\sigma} u) = \iota\bar{\sigma}[v, x] \\
&= \iota([\bar{\sigma} v, x] + [v, \bar{\sigma} x]) \\
&= [\iota\bar{\sigma} v, x] + \iota[v, x] \\
&= (n-1)\,\iota[v, x] + \iota[v, x] \\
&= (n-1)\,\iota u + \iota u = (n-1)\,a + a = na. \quad \square
\end{aligned}$$

Proposition 2 implies that if $a = \iota u$, then

$$u = \frac{\sigma a}{n}.$$

By statement B the condition $a = \iota u$ holds for $a = z_n(x, y)$ and $u = \mathfrak{z}_n(x, y)$. Consequently

$$\mathfrak{z}_n(x, y) = \frac{\sigma z_n(x, y)}{n},$$

i.e. (see formula (2))

$$\text{(8)} \qquad \mathfrak{z}_n(x, y) = \frac{1}{n} \sum_{k=1}^{n} \frac{(-1)^{k-1}}{k} \sum_{(p)(q)} \frac{\sigma(x^{p_1} y^{q_1} \ldots x^{p_k} y^{q_k})}{p_1!\, q_1! \ldots p_k!\, q_k!},$$

where the summation in the internal sum is taken over all integral nonnegative exponents $p_1, q_1, \ldots, p_k, q_k$ such that

$$p_1 + q_1 > 0, \ \ldots, \ p_k + q_k > 0$$

and

$$p_1 + q_1 + \ldots + p_k + q_k = n.$$

This is the formula we wanted to obtain.

For a Lie formal series

$$\mathfrak{H}(x, y) = \sum_{n=1}^{\infty} \mathfrak{H}_n(x, y) \tag{9}$$

after the regrouping of the terms we get

$$\mathfrak{H}(x, y) = \sum_{k=1}^{\infty} \sum_{(p),\,(q)} \frac{(-1)^{k-1}}{k} \frac{1}{p_1+q_1+\dots+p_k+q_k} \times \frac{[x^{p_1}y^{q_1}\dots x^{p_k}y^{q_k}]}{p_1!\,q_1!\dots p_k!\,q_k!}, \tag{10}$$

where for the sake of vivid presentation $\sigma(x^{p_1}y^{q_1}\dots x^{p_k}y^{q_k})$ is replaced by $[x^{p_1}y^{q_1}\dots x^{p_k}y^{q_k}]$.

That series is called a *Campbell-Hausdorff series in the Dynkin form.*

Series (10) is inconvenient for practical calculations since it contains many ungrouped like terms. The difficulty of grouping those terms is well illustrated by an example of calculating a part of series (10) linear in x.

A Lie monomial $[x^{p_1}y^{q_1}\dots x^{p_m}y^{q_m}]$ is linear in x (and nonzero) if and only if either $p_1 = 1, p_2 = 0, \dots, p_m = 0$ (and it is only that monomial that is of the form $[xy^n]$ where $n = q_1 + \dots + q_m$) or $p_1 = 0$, $p_2 = 1$, $p_3 = 0, \dots, p_m = 0$, $q_1 = 1$ (and then it is of the form $[yxy^{n-1}]$, where $n - 1 = q_2 + \dots + q_m$), with $q_1 \geqslant 0, q_2 \geqslant 1, \dots, q_m \geqslant 1$ in the former case and $q_2 \geqslant 0, q_3 \geqslant 1, \dots, q_m \geqslant 1$ in the latter. Since $[yxy^{n-1}] = -[xy^n]$ we thus see, somewhat changing the notation, that the part of $\mathfrak{H}(x, y)$ linear in x (we denote it by $\mathfrak{H}'(x, y)$) can be expressed as follows:

$$\mathfrak{H}'(x, y) = \sum_{m=1}^{\infty} \frac{(-1)^{m-1}}{m} \sum_{n=m-1}^{\infty} \frac{1}{n+1} \times \left(\sum{}' \frac{1}{q_1!\,q_2!\dots q_m!} - \sum{}'' \frac{1}{q_1!\,q_2!\dots q_{m-1}!} \right) [xy]^n,$$

where the summation in $\sum'$ is taken over all the sets of integers $q_1, q_2, \dots, q_m$ such that

$$q_1 \geqslant 0,\ q_2 \geqslant 1, \dots,\ q_m \geqslant 1 \text{ and } q_1 + q_2 + \dots + q_m = n$$

and the summation in $\sum''$ is taken over integers $q_1, q_2, \ldots, q_{m-1}$ such that

$$q_1 \geqslant 0, \ q_2 \geqslant 1, \ \ldots, \ q_{m-1} \geqslant 1$$

and

$$q_1 + q_2 + \ldots + q_{m-1} = n - 1.$$

When $m = 1$ there is no sum $\sum''$.

To calculate the coefficients of $\mathfrak{D}'(x, y)$ we make use of the standard method of generating functions. Let $A(t)$ be a series obtained from $\mathfrak{D}'(x, y)$ by replacing $[xy^n]$ by t^n. Since

$$\sum_{n=m-1}^{\infty} \sum{}' \frac{1}{q_1! q_2! \ldots q_m!} \frac{t^n}{n+1}$$

$$= \frac{1}{t} \sum_{n=m-1}^{\infty} \int_0^t dt \sum{}' \frac{1}{q_1!\, q_2! \ldots q_m!} t^n$$

$$= \frac{1}{t} \int_0^t dt \left(\sum_{q_1=0}^{\infty} \frac{t^{q_1}}{q_1!} \right) \left(\sum_{q_2=1}^{\infty} \frac{t^{q_2}}{q_2!} \right)^{m-1}$$

$$= \frac{1}{t} \int_0^t e^t (e^t - 1)^{m-1}\, dt$$

and similarly

$$\sum_{n=m-1}^{\infty} \sum{}'' \frac{1}{q_1!\, q_2! \ldots q_{m-1}!} \frac{t^n}{n+1} = \frac{1}{t} \int_0^t te^t (e^t - 1)^{m-2}\, dt,$$

we have

$$A(t) = \frac{1}{t} \int_0^1 \frac{e^t}{e^t - 1} \left(\sum_{m=1}^{\infty} \frac{(-1)^{m-1}}{m} (e^t - 1)^m \right) dt$$

$$- \frac{1}{t} \int_0^t \frac{te^t}{(e^t - 1)^2} \left(\sum_{m=2}^{\infty} \frac{(-1)^{m-1}}{m} (e^t - 1)^m \right) dt$$

$$=\frac{1}{t}\int_0^t \frac{e^t}{e^t-1}\,t\,dt-\frac{1}{t}\int_0^t \frac{te^t}{(e^t-1)^2}\,(t-(e^t-1))\,dt$$

$$=\frac{te^t}{e^t-1}=\frac{-t}{e^{-t}-1}=\sum_{n=0}^{\infty}\frac{B_n}{n!}(-t)^n,$$

where B_n are the so-called Bernoulli numbers. Since $[xy^n]=(-\mathrm{ad}\,y)^n x$, this proves that

$$\mathfrak{H}'(x, y)=\sum_{n=0}^{\infty}\frac{B_n}{n!}(\mathrm{ad}\,y)^n x=\frac{\mathrm{ad}\,y}{e^{\mathrm{ad}\,y}-1}\,x,$$

i.e. (since the only term of $\mathfrak{H}(x, y)$ containing no x is y), that

(11) $$\mathfrak{H}(x, y)=y+\frac{\mathrm{ad}\,y}{e^{\mathrm{ad}\,y}-1}\,x+\ldots,$$

where the dots represent terms of at least second degree in x.

It can be similarly shown that

(12) $$\mathfrak{H}(x, y)=x+\frac{-\mathrm{ad}\,x}{e^{-\mathrm{ad}\,x}-1}\,y+\ldots,$$

where the dots represent terms of at least second degree in y.

We now investigate the convergence of series (9) and (10). To do this we use Lemma 1 of Lecture 2 which, as was noted, applies to any finite-dimensional algebras and in particular to an arbitrary finite-dimensional Lie algebra $\mathfrak{g}$.

Let $\|\ \|$ be a multiplicative norm in $\mathfrak{g}$ and let X and Y be elements in $\mathfrak{g}$ such that $\|X\|<\delta$ and $\|Y\|<\delta$ where $0<\delta<1$.

Since $\mathfrak{l}\langle x, y\rangle$ is a free algebra, there is a unique homomorphism $\mathfrak{l}\langle x, y\rangle\to\mathfrak{g}$ sending elements x and y to elements X and Y. The image under that homomorphism of an element $u=u(x, y)$ of $\mathfrak{l}\langle x, y\rangle$ will be denoted by $u(X, Y)$.

An obvious induction (using the multiplicity of the norm) now shows that if u is a Lie monomial of degree n, then

$$\|u(X, Y)\|\leqslant\delta^n.$$

It follows that if $u = \sum c_\alpha u_\alpha$ where u_α are Lie monomials of degree n, then

$$\| u(X, Y) \| \leqslant C\delta^n,$$

where $C = \sum\limits_\alpha | c_\alpha |$. In particular we get (see (8))

$$\| \mathfrak{H}_n (X, Y) \| \leqslant D_n \delta^n, \tag{13}$$

where

$$D_n = \frac{1}{n} \sum_{k=1}^{n} \frac{1}{k} \sum_{(p),\,(q)} \frac{1}{p_1!\, q_1! \ldots p_k!\, q_k!}.$$

The internal sum in the last formula is equal in value to the coefficient of t^n in the Maclaurin series of the function $(e^{2t} - 1)^k$. The number nD_n is therefore equal to the coefficient of t^n in the Maclaurin series of the function $\sum\limits_{k=1}^{n} \frac{1}{k} \times (e^{2t} - 1)^k$ or equivalently of the function

$$f(t) = \sum_{k=1}^{\infty} \frac{1}{k} (e^{2t} - 1)^k.$$

Hence

$$\sum_{n=1}^{\infty} D_n \delta^n = \int_0^{\delta} \frac{f(t)}{t}\, dt. \tag{14}$$

Since the series for $f(t)$ obviously converges if $| e^{2t} - 1 | < 1$ and hence if $| t | < \frac{\ln 2}{2}$, this proves that *series* (14) *converges if* $\delta < \frac{\ln 2}{2}$. Since by formula (13) series (14) majorizes to the series

$$\mathfrak{H}(X, Y) = \sum_{n=1}^{\infty} \mathfrak{H}_n (X, Y) \tag{15}$$

it follows that *series* (15) *converges if* $\| X \| < \delta_0$, $\| Y \| < \delta_0$ *where* $\delta_0 = \frac{\ln 2}{2}$. □

Remark 1. The convergence of series (15), with $\| X \| < \delta_0$, $\| Y \| < \delta_0$, has already been proved in Lecture 4. The only new fact is that now the convergence of (15) is proved for any (finite-dimensional) Lie algebra $\mathfrak{g}$ whereas in Lecture 5 the algebra $\mathfrak{g}$ was assumed to be a Lie algebra of some Lie (local) group.

Suppose again that G is an analytic (or local) Lie group and that $\mathfrak{g} = \mathfrak{l}(G)$ is its Lie algebra. Since the exponential mapping exp is a diffeomorphism at a point $0 \in \mathfrak{g}$, it allows us to take (using the formula $X \cdot Y = \exp^{-1}(\exp X \cdot \exp Y)$) the multiplication we have in G to some neighbourhood of zero of the algebra $\mathfrak{g}$. Thus the vector space $\mathfrak{g}$ is turned into a local Lie group isomorphic (in the category GR-LOC) to the local group G (the isomorphism is realized by the mapping exp).

Thus in addition to linear operations and the Lie operation $X, Y \mapsto [X, Y]$ the vector space $\mathfrak{g}$ contains yet another operation ("multiplication") relative to which the space $\mathfrak{g}$ is a local Lie group. That operation is connected with the operations in the Lie algebra $\mathfrak{g}$ as follows:

$$X \cdot Y = \mathfrak{H}(X, Y).$$

The constructed object deserves a special definition.

Definition 2. A *Lie group algebra* is a finite-dimensional space $\mathfrak{g}$ over $\mathbb{R}$ which is at the same time a Lie algebra (with a multiplication $[x, y]$) and a local Lie group (with a multiplication xy) in which the product xy is defined if and only if the Campbell-Hausdorff series $\mathfrak{H}(x, y)$ converges and in that case coincides with its sum:

$$xy = \mathfrak{H}(x, y).$$

It follows immediately from (11) and (12) that for any element X (sufficiently close to zero) of a Lie group algebra $\mathfrak{g}$ differentials $(dL_X)_0$ and $(dR_Y)_0$ at the point 0 of the shifts $L_X\colon Y \mapsto \mathfrak{H}(X, Y)$ and $R_Y\colon X \mapsto \mathfrak{H}(X, Y)$ are defined as follows:

$$(dL_X)_0 = \frac{-\operatorname{ad} X}{e^{-\operatorname{ad} X} - E}, \quad (dR_X)_0 = \frac{e^{\operatorname{ad} X}}{e^{\operatorname{ad} X} - E}.$$

Remark 2. We have already proved the second of these formulas by another method in Lecture 4 (see Corollary 1 to Proposition 3, Lecture 4).

The mapping $\mathfrak{g} \to \mathfrak{h}$ of Lie group algebras is said to be a *homomorphism* if it is their homomorphism as Lie algebras (and hence as local Lie groups).

It is clear that all Lie group algebras and all their homomorphisms form a category. This will be denoted by GRIE.

According to the foregoing every local Lie group G can be associated with some Lie group algebra by carrying over with the aid of the exponential mapping exp the multiplication on G into $\mathfrak{g}$. That Lie group algebra will be denoted by $\mathfrak{l}'(G)$. It is clear that the correspondence $G \mapsto \mathfrak{l}'(G)$ is some functor

$$\mathfrak{l}': \text{GR-LOC} \to \text{GRIE}.$$

This will also be called a *Lie functor*.

Consider now the *forgetful functor*

$$I: \text{GRIE} \to \text{GR-LOC}$$

whose action consists in discarding (forgetting) in every Lie group algebra its Lie algebra structure.

On the face of it, it seems that the functors $\mathfrak{l}'$ and I are mutually inverse. This is not the case, however. Indeed, for an arbitrary local Lie group G the local group $(I \circ \mathfrak{l}')\, G$ is not a local group G but the local group on a vector space $\mathfrak{l}(G)$ constructed above, which is distinct, in general from the local group G. Nevertheless we can see that the last local group is naturally isomorphic to the local group G (the corresponding isomorphism is the exponential mapping exp). In terms of functor theory this means that the *functor* $I \circ \mathfrak{l}'$ *is isomorphic to the identity functor* Id *of the category* GR-LOC:

$$I \circ \mathfrak{l} \approx \mathrm{Id}.$$

Similarly *the functor* $\mathfrak{l}' \circ I$ *is isomorphic to the identity functor* Id of *the category* GRIE:

$$\mathfrak{l}' \circ I \approx \mathrm{Id}.$$

Indeed the functor $\mathfrak{l}' \circ I$ associates with a Lie group algebra $\mathfrak{g}$ a group algebra that coincides as a vector space with a tangent space $\mathbf{T}_0(\mathfrak{g})$. But we know that there is a natural isomorphism

$$l: \mathfrak{g} \to \mathbf{T}_0(\mathfrak{g})$$

between the vector spaces $\mathfrak{g}$ and $\mathsf{T}_0(\mathfrak{g})$. We show that l is an isomorphism of Lie group algebras.

By definition the isomorphism l sends an element $x \in \mathfrak{g}$ to the tangent vector to a curve $t \mapsto tx$ at the point 0. Since $(tx)\cdot(sx) = \mathfrak{H}(tx, sx) = \mathfrak{H}_1(tx, sx) = (t+s)x$, that curve is a one-parameter subgroup of a local Lie group $I\mathfrak{g}$ and therefore (see Proposition 1, Lecture 4) for any two elements x, $y \in \mathfrak{g}$ the vector $[lx, ly]$ is the tangent vector to a curve at the point 0

$$t \mapsto (\sqrt{t}x)(\sqrt{t}y)(\sqrt{t}x)^{-1}(\sqrt{t}y)^{-1}.$$

But since (see the proof of Proposition 1, Lecture 4)

$$(\sqrt{t}x)(\sqrt{t}y)(\sqrt{t}x)^{-1}(\sqrt{t}y)^{-1} = t[x, y] + O(t^{3/2})$$

that curve has at the point 0 the same tangent vector as the curve $t \mapsto t[x, y]$. Consequently

$$[lx, ly] = l[x, y]$$

so that l is indeed an isomorphism of Lie algebras and hence of Lie group algebras. $\square$

If functors F: $\mathsf{C} \to \mathsf{D}$ and G: $\mathsf{D} \to \mathsf{C}$ where C and D are some categories, have the property that the composite functors $F \circ G$ and $G \circ F$ are isomorphic to the identity functors (of D and C respectively), then F and G are said to be *quasi-inverse*. Categories C and D for which there are quasi-inverse functors $\mathsf{C} \to \mathsf{D}$ and $\mathsf{D} \to \mathsf{C}$ are called *equivalent*.

We have thus proved the following proposition:

Proposition 3. *Categories* GR-LOC *and* GRIE *are equivalent. The equivalence is realized by the quasi-inverse functors* $\mathfrak{l}$ *and* I. $\square$

Discarding in a Lie group algebra the local Lie group structure we obtain the forgetful functor

$$J\colon \text{GRIE} \to \text{ALG}_f\text{-LIE}$$

whose composition $J \circ \mathfrak{l}'$ with the Lie functor $\mathfrak{l}'$: GR-LOC $\to$ GRIE is nothing but the Lie functor, which is of primary interest to us,

$$\mathfrak{l}\colon \text{GR-LOC} \to \text{ALG}_f\text{-LIE}$$

for local groups.

Proposition 4. *For the functor* J *there is an inverse functor*

$$J^{-1}\colon \text{ALG}_f\text{-LIE} \to \text{GRIE}.$$

Proof. Let $\mathfrak{g}$ be an arbitrary Lie algebra (in which multiplication is denoted by $[x, y]$). If the group algebra $J^{-1}\mathfrak{g}$ exists, then as Lie algebra it coincides with the algebra $\mathfrak{g}$ and multiplication in it is connected with the operations in $\mathfrak{g}$ as follows:

$$xy = \mathfrak{H}(x, y).$$

To prove Proposition 3 therefore it suffices to establish that for any Lie algebra $\mathfrak{g}$ that formula defines in $\mathfrak{g}$ a multiplication which satisfies the axioms of local Lie groups. To do this it suffices in turn to prove that:

(a) there is a neighbourhood of zero U in $\mathfrak{g}$ such that for $x, y \in U$ the series $\mathfrak{H}(x, y)$ converges;

(b) the mapping $U \times U \to \mathfrak{g}$ defined by the correspondence $x, y \mapsto \mathfrak{H}(x, y)$ together with the mapping $x \mapsto x^{-1} = -x$, has the properties enumerated in Definition 1 of Lecture 4.

Statement (a) has already been proved above, and to prove (b) first notice that in the algebra of formal series in three noncommuting unknowns x, y, z we have

$$(e^x e^y)\, e^z = e^x\, (e^y e^z)$$

(a formula that can be verified by direct manipulation). Since the substitution $[x, y] \mapsto xy - yx$ turns the Campbell-Hausdorff series $\mathfrak{H}(x, y)$ into a series $\ln(e^x e^y)$, it follows immediately that the multiplication $x, y \mapsto \mathfrak{H}(x, y)$ is associative (provided all the necessary series converge). Similarly since $\mathfrak{H}(0, x) = \mathfrak{H}(x, 0) = 0$, the multiplication $x, y \mapsto \mathfrak{H}(x, y)$ has the identity 0, and since $e^x e^{-x} = 1$ the inverse element x^{-1} relative to that multiplication is the element $-x$.

This completes the proof of Proposition 4. $\square$

Since the functor I is the quasi-inverse of $\mathfrak{l}'$, the functor $E = I \circ J^{-1}$ is the quasi-inverse of the Lie functor $\mathfrak{l} = J \circ \mathfrak{l}'$. Thus we have attained our main object: we have found a functor which, if not the inverse, is the quasi-inverse of the Lie functor GR-LOC $\to$ ALG_f-LIE.

All the results obtained can be summarized in the following final theorem:

Theorem 1. *There is the following commutative diagram of functors*

$$\begin{tikzcd}
\text{GR-LOC} \arrow[rr, shift left, "\mathfrak{I}"] \arrow[dr, shift left, "\mathfrak{I}'"] & & \text{ALG}_f\text{-LIE} \arrow[ll, shift left, "E"] \arrow[dl, shift left, "J^{-1}"] \\
& \text{GRIE} \arrow[ul, shift left, "I"] \arrow[ur, shift left, "J"] &
\end{tikzcd}$$

in which the functors J and J^{-1} are inverse and the functors $\mathfrak{I}$ and E and $\mathfrak{I}'$ and I are quasi-inverse to each other. □

Corollary. *Categories* GR-LOC, ALG$_f$-LIE *and* GRIE *are equivalent.* □

Theorem 1 was basically known to Sophus Lie.

Lie presented his results as six theorems: three direct theorems and three converses of the theorems. His third converse theorem is almost the same as Theorem 1. On these rather shaky grounds theorem 1 is sometimes referred to as *Lie's third theorem.*

We stress that in Theorem 1 local Lie groups are assumed to be *analytic*. The case of local groups belonging to the class of C^r smoothness, $2 \leqslant r \leqslant \infty$, will be considered in the next lecture.

Lecture 7

Local subgroups and subalgebras • Invariant local subgroups and ideals • Local factor groups and quotient algebras • Reducing smooth local groups to analytic ones • Pfaffian systems • Subfiberings of tangent bundles • Integrable subfiberings • Graphs of a Pfaffian system • Involutory subfiberings • The complete univalence of a Lie functor • The involutedness of integrable subfiberings • Completely integrable subfiberings

Theorem 1 of the preceding lecture completely reduces the theory of (analytic) local Lie groups to the theory of Lie algebras. We illustrate this by using the example of local subgroups and local factor groups.

Definition 1. A *local subgroup* of a local Lie group G is its subset H such that:

(i) if for elements a, $b \in H$ an element ab^{-1} is defined, then $ab^{-1} \in H$;

(ii) there is a neighbourhood U of the identity e of G such that the intersection $U \cap H$ is closed in U (*the condition of local closure*).

Notice that it is not immediately apparent from this definition that the local subgroup H is itself a local Lie group (although we shall see below that it is really the case).

Let $\mathfrak{g}$ be a Lie algebra and let $\mathfrak{h}$ be some subalgebra of it. Using the functor $E = I \circ J^{-1}$ we can construct from $\mathfrak{g}$ a local Lie group $E\mathfrak{g}$ and from $\mathfrak{h}$ a local Lie group $E\mathfrak{h}$. According to the construction, $E\mathfrak{h}$ is a subset of $E\mathfrak{g}$ and what is more, its local subgroup (for if $x, y \in \mathfrak{h}$, then $\mathfrak{H}_n(x, y) \in \mathfrak{h}$ for any $n \geqslant 1$).

Now let G be a local Lie group and let $\mathfrak{g} = \mathfrak{l}(G)$ be its Lie algebra. Under natural isomorphism $E\mathfrak{g} \approx G$ every

local subgroup of $E\mathfrak{g}$, which is of the form $E\mathfrak{h}$, where $\mathfrak{h}$ is a subalgebra of $\mathfrak{g}$, is associated with some local subgroup of G. In some neighbourhood of the identity $e \in G$ that local subgroup coincides, under the exponential mapping exp, with the image $\exp \mathfrak{h}$ of $\mathfrak{h}$, so that by our convention not to distinguish between equivalent local groups we may denote it by $\exp \mathfrak{h}$.

The local subgroup $\exp \mathfrak{h}$ of G corresponding to the subalgebra $\mathfrak{h}$ of $\mathfrak{g} = \mathfrak{l}(G)$ has the property that in some system of normal coordinates $x^1, \ldots, x^n$ (namely in the system defined by the basis of $\mathfrak{g}$ whose first m vectors form the basis of $\mathfrak{h}$) it is given by linear equations

$$x^{m+1} = 0, \ldots, x^m = 0. \tag{1}$$

Local subgroups having that property will be said to be *locally flat*. Thus for a local subgroup $H \subset G$ to be of the form $\exp \mathfrak{h}$ it is necessary that it should be locally flat. It is easy to see, however, that this necessary condition is also sufficient, so that a *local subgroup H of a local Lie group G is associated with some subalgebra of a Lie algebra $\mathfrak{g} = \mathfrak{l}(G)$* (and is therefore, in particular, itself a local Lie group) *if and only if it is locally flat*. Indeed, let $\mathfrak{h}$ be a subspace of $\mathfrak{g}$ spanned by the first m vectors of the basis defining normal coordinates in which H is given by equations (1). Then for any $X \in \mathfrak{h}$ and any t (with $|t|$ sufficiently small) the point $\beta_X(t) = \exp tX$ is in H. Therefore if $X, Y \in \mathfrak{h}$, then

$$\beta(t) = \beta_X(\sqrt{t})\beta_Y(\sqrt{t})\beta_X(\sqrt{t})^{-1}\beta_Y(\sqrt{t})^{-1} \in H$$

and hence the vector

$$[X, Y] = \left.\frac{d\beta(t)}{dt}\right|_{t=0}$$

(see Proposition 2, Lecture 4) is in $\mathfrak{h}$. Consequently $\mathfrak{h}$ is a subalgebra of $\mathfrak{g}$. To complete the proof it remains to notice that the local groups H and $E\mathfrak{h}$ are obviously equivalent. $\square$

We see in particular that for a locally flat local subgroup H a subalgebra $\mathfrak{h} \subset \mathfrak{l}(G)$ consists of all elements $X \in \mathfrak{l}(G)$ for which $\exp tX \in H$ for any t (with $|t|$ sufficiently small). That subalgebra is naturally identified with a Lie algebra $\mathfrak{l}(H)$ of H (considered as a local Lie group) and will be denoted by the same symbol $\mathfrak{l}(H)$.

Thus *for any local Lie group G there is a bijective correspondence between the set of all subalgebras of a Lie algebra $\mathfrak{g} = \mathfrak{l}(G)$ and the set of all locally flat local subgroups of G in which a subalgebra $\mathfrak{h} \subset \mathfrak{g}$ has the corresponding local subgroup* $\exp \mathfrak{h}$ *and a local subgroup $H \subset G$ has the corresponding subalgebra* $\mathfrak{l}(H)$.

That correspondence will be called the *Lie correspondence.*

The remarkable fact, first proved by E. Cartan, is that the condition that local subgroups should be locally flat is in fact unnecessary in that statement.

Proposition 1 (The Cartan theorem). *Every local subgroup H of a local Lie group G is locally flat and hence the Lie algebra $\mathfrak{g} = \mathfrak{l}(G)$ has a subalgebra $\mathfrak{h}$ such that*

$$H = \exp \mathfrak{h}.$$

In particular H is a local Lie group.

Proof. Let $\mathfrak{h}$ be the collection of all elements $X \in \mathfrak{g}$ having the property that $\exp tX \in H$ for any t (with sufficiently small $|t|$). We prove that $\mathfrak{h}$ is a subalgebra of $\mathfrak{g}$ and that $\exp \mathfrak{h} = H$. The proof is split into several lemmas.

Lemma 1. *If for an element $X \in \mathfrak{g}$ there is a sequence $\{X_i\}$ converging to X such that for some $t_i \in \mathbb{R}$ vanishing as $i \to \infty$ we have an inclusion*

$$\exp t_i X_i \in H,$$

then $X \in \mathfrak{h}$.

Proof. Since $\Pi \exp(-t_i X_i) = \Pi \exp(t_i X_i)^{-1} \in H$, it may be assumed without loss of generality that $t_i > 0$. Let $t > 0$ be a number such that the element $\exp tX \in G$ is defined and let

$$k_i(t) = \left[\frac{t}{t_i}\right) \left(\text{the integral part of } \frac{t}{t_i}\right).$$

Since $\frac{t}{t_i} - 1 < k_i(t) \leqslant \frac{t}{t_i}$, we have $\lim\limits_{t \to \infty} t_i k_i(t) = t$ and hence

$$\lim_{t \to \infty} \exp(t_i k_i(t) X_i) \exp tX.$$

But

$$\exp(t_i k_i(t) X_i) = (\exp t_i X_i)^{k_i(t)} \in H$$

and under the hypothesis the local subgroup H is closed. Consequently $\exp tX \in H$ and hence $X \in \mathfrak{h}$. □

Lemma 2. *A subset $\mathfrak{h} \subset \mathfrak{g}$ is a subalgebra.*

Proof. Since $\exp(t(sX)) = \exp((ts)X)$, for any $X \in \mathfrak{h}$ and any $s \in \mathbb{R}$ there is an inclusion $sX \in \mathfrak{h}$ (for we can always choose sufficiently small t).

Let $X, Y \in \mathfrak{h}$. Then exp د $(tX, tY) = \exp tX \cdot tY \in H$, i.e. $\exp t(X + Y + Z_t) \in H$, where $Z_t = O(t)$. On arbitrarily choosing a sequence $\{t_i\}$ converging to zero, we set $X_i = X + Y + Z_{t_i}$. The sequence $\{X_i\}$ satisfies (with respect to the element $X + Y$) all the conditions of Lemma 1. Therefore by that lemma $X + Y \in \mathfrak{h}$.

Similarly, since

$$\begin{aligned} \exp tX \cdot \exp tY \cdot (\exp tX)^{-1} (\exp tY)^{-1} \\ = \exp t^2 ([X, Y] + O(t)) \in H, \end{aligned}$$

we have $[X, Y] \in \mathfrak{h}$. □

Now let $\mathfrak{t}$ be a subspace of a Lie algebra $\mathfrak{g}$ complementary to a subalgebra $\mathfrak{h}$, i.e. such that

$$\mathfrak{g} = \mathfrak{h} \oplus \mathfrak{t}. \tag{2}$$

Lemma 3. *There is a neighbourhood V of zero in $\mathfrak{t}$ such that*

$$\exp Y \notin H$$

for any nonzero element $Y \in \mathfrak{t}$.

Proof. On choosing in $\mathfrak{t}$ some norm $\|\mathfrak{t}\|$ (say a Euclidean one) consider the set B of all elements $Y \in \mathfrak{t}$ such that $1 \leqslant \|Y\| \leqslant 2$. If Lemma 3 is false, then there is a sequence $Y_i \to 0$ in the algebra $\mathfrak{g}$ such that $Y_i \in \mathfrak{t}$ and $\exp Y_i \in H$. We choose integers n_i so that $X_i = n_i Y_i \in B$ (it is clear that this is always possible). Since B is compact, it may be assumed without loss of generality that $\{X_i\}$ converges. Let X be its limit. Since $\{X_i\}$ satisfies all the conditions of Lemma 1 (with $t_i = 1/n_i$), the element X (obviously nonzero) is in the subalgebra $\mathfrak{h}$. But this is impossible, since $X \in \mathfrak{t}$ and $\mathfrak{h} \cap \mathfrak{t} = 0$. Hence the statement of Lemma 3 cannot be false. □

Lemma 4. *In a local Lie group G there is an equation*

$$H = \exp \mathfrak{h}.$$

Proof. Since by construction $\exp \mathfrak{h} \subset H$, it is only necessary to show that the inverse inclusion holds. It may be assumed without loss of generality that the local group G is the canonical neighbourhood of the identity, which corresponds to decomposition (2) of the algebra $\mathfrak{g}$ (see Definition 4, Lecture 5). Moreover, we may assume that G is the image under the mapping

$$X + Y \mapsto \exp X \cdot \exp Y, \; X \in \mathfrak{h}, \; Y \subset \mathfrak{t},$$

of the neighbourhood of zero in $\mathfrak{g}$, the neighbourhood being of the form $U \oplus V$, where U is some neighbourhood of zero in $\mathfrak{h}$ and V is a neighbourhood of zero in $\mathfrak{t}$ stipulated in Lemma 3. But under these conditions the inclusion $\exp \mathfrak{h} \supset H$ is obvious since if $\exp X \cdot \exp Y \in H$, then $\exp Y \in H$ (since $\exp X \in H$) and hence $Y = 0$ by Lemma 3. □

This completes the proof of Proposition 1. □

Corollary. *The Lie correspondence is a natural bijective correspondence between the set of all local Lie subgroups of a local Lie group G and the set of all subalgebras of a Lie algebra $\mathfrak{g} = \mathfrak{l}(G)$.* □

On noticing that with respect to the inclusion both of these sets are lattices (structures) it immediately follows that the *Lie correspondence is an isomorphism of those lattices.*

Definition 2. A local subgroup H of a local Lie group G is said to be *invariant* or distinguished if $aba^{-1} \in H$ for any elements $a \in G$ and $b \in H$ such that the element aba^{-1} is defined.

Definition 3. A subalgebra $\mathfrak{h}$ of a Lie algebra $\mathfrak{g}$ is said to be *an ideal* if $[X, Y] \in \mathfrak{h}$ for any elements $X \in \mathfrak{g}$ and $Y \in \mathfrak{h}$.

Proposition 2. *In the Lie correspondence the invariant local subgroups of a local group G are associated with the ideals of a Lie algebra $\mathfrak{g} = \mathfrak{l}(G)$ and the ideals with the invariant local subgroups.*

Proof. Let $\mathfrak{h}$ be an ideal of $\mathfrak{g} = \mathfrak{l}(G)$ and let $X \in \mathfrak{g}$, and $Y \in \mathfrak{h}$. Since $[X, Y] \in \mathfrak{h}$, it immediately follows that $\mathfrak{Z}_n(X, Y) \in \mathfrak{h}$ for any $n > 1$ and therefore

$$\mathfrak{Z}(X, Y) = X + Y^*,$$

where $Y^* = Y + \sum_{n>1} \mathfrak{Z}_n(X, Y) \in \mathfrak{h}$ (if, of course, the series $\mathfrak{Z}(X, Y)$ converges). Since $[X + Y^*, -X] = [X, Y^*] \in$

$\mathfrak{h}$ and hence $\mathcal{H}_n\,(X + Y^*,\ -X) \in \mathfrak{h}$ for $n > 1$, it follows that

$$\mathcal{H}\,(\mathcal{H}\,(X,\ Y),\ -X) = X + Y^* - X + \sum_{n>1} \mathcal{H}_n\,(X+Y^*,\ -X)$$

$\in \mathfrak{h}$, and therefore

$$\exp X \cdot \exp Y \cdot (\exp X)^{-1} = \exp \mathcal{H}\,(\mathcal{H}\,(X,\ Y),\ -X) \in \exp \mathfrak{h}.$$

Consequently the local subgroup $\exp \mathfrak{h}$ is invariant.

Conversely, let $H = \exp \mathfrak{h}$ be an invariant local subgroup of a local Lie group G. Then for any elements $X \in \mathfrak{g}$, $Y \in \mathfrak{h}$ and any t (with $|\,t\,|$ sufficiently small) there is an inclusion

$$\exp tX \cdot \exp tY \cdot (\exp tX)^{-1} \in H$$

and therefore an inclusion

$$\exp tX \cdot \exp tY \cdot (\exp tX)^{-1} \cdot (\exp tY)^{-1}$$
$$= \exp t^2\,([X,\ Y] + O\,(t)) \in H$$

from which by the already familiar reasoning (see the proof of Lemma 2 above) we get $[X,\ Y] \in \mathfrak{h}$. Hence the subalgebra $\mathfrak{h} = \mathfrak{l}\,(H)$ is an ideal. □

Let H be a local subgroup of a local Lie group G. We call $a, b \in G$ elements *comparable modulo* H if $a^{-1}b \in H$. It is clear that on a sufficiently small neighbourhood of the identity of G that relation is an equivalence relation whose equivalence classes are cosets aH (more exactly, the intersections of those sets with a neighbourhood of the identity). Let G/H be the set of the cosets.

On decomposing the Lie algebra $\mathfrak{g} = \mathfrak{l}\,(G)$ into a direct sum $\mathfrak{g} = \mathfrak{h} \oplus \mathfrak{k}$ of a Lie algebra $\mathfrak{h}$ of a local subgroup H and some subspace $\mathfrak{k}$ and considering the canonical coordinates $x^1, \ldots, x^n$ defined by the decomposition we at once see that the cosets $aH \in G/H$ are given in the coordinates $x^1, \ldots, x^n$ by equations of the form

(3) $\quad x^{m+1} = a^1, \ \ldots, \ x^n = a^{n-m} \ (n = \dim G, m = \dim H),$

where $a^1, \ldots, a^{n-m}$ are arbitrary real numbers (sufficiently small in absolute value). This shows that by associating a point $(a^1, \ldots, a^{n-m}) \in \mathbb{R}^{n-m}$ with a coset aH we obtain some bijective mapping of the set G/H onto an open subset of the space $\mathbb{R}^{n-m}$, i.e. we obtain a chart. Since with a dif-

ferent choice of complementary subspace $\mathfrak{k}$ a compatible chart is easily seen to result, this defines on G/H a topology and smoothness relative to which it is a smooth manifold (diffeomorphic to some open subset of $\mathbb{R}^{n-m}$ and having therefore the dimension $n-m$).

If H is an invariant local subgroup, then the formula $aH \cdot bH = abH$ correctly defines in the neighbourhood of a point $H = eH$ of the manifold G/H a certain multiplication relative to which it is obviously a local Lie group with identity H.

Definition 4. The constructed local Lie group G/H is called a *local factor group* of a local Lie group G mod an invariant local subgroup H.

Now let $\mathfrak{h}$ be an ideal of some Lie algebra $\mathfrak{g}$. Consider a factor space $\mathfrak{g}/\mathfrak{h}$ whose elements are cosets $x + \mathfrak{h}$, $x \in \mathfrak{g}$. It is obvious that the formula

$$[x + \mathfrak{h},\ y + \mathfrak{h}] = [x,\ y] + \mathfrak{h}$$

correctly defines on $\mathfrak{g}/\mathfrak{h}$ the operation $[\ ,\ ]$ relative to which that factor space is a Lie algebra.

Definition 5. A Lie algebra $\mathfrak{g}/\mathfrak{h}$ is called a *quotient algebra* of a Lie algebra $\mathfrak{g}$ mod an ideal $\mathfrak{h}$.

In particular, for any invariant local subgroup H of a local Lie group G a quotient algebra $\mathfrak{l}(G)/\mathfrak{l}(H)$ of a Lie algebra $\mathfrak{l}(G)$ mod its ideal $\mathfrak{l}(H)$ is defined. We compare that quotient algebra with the Lie algebra $\mathfrak{l}(G/H)$ of a local factor group G/H.

Proposition 3. *Lie algebras* $\mathfrak{l}(G/H)$ *and* $\mathfrak{l}(G)/\mathfrak{l}(H)$ *are naturally isomorphic*:

$$\mathfrak{l}(G/H) \approx \mathfrak{l}(G)/\mathfrak{l}(H).$$

Proof. On applying to $\mathfrak{l}(G/H)$ and $\mathfrak{l}(G)/\mathfrak{l}(H)$ the functor E: ALG_f-LIE $\to$ GR-LOC, on the one hand we obtain a local Lie group $E(\mathfrak{l}(G/H))$ which is naturally isomorphic to the local group G/H and on the other hand we obtain a local Lie group $E(\mathfrak{l}(G)/\mathfrak{l}(H))$. Proposition 3 therefore is equivalent to the statement that we have a natural isomorphism

$$G/H \approx E(\mathfrak{l}(G)/\mathfrak{l}(H)).$$

It is in this form that we shall prove it.

Let $\mathfrak{g} = \mathfrak{l}\,(G)$ and $\mathfrak{h} = \mathfrak{l}\,(H)$. Elements of the local group $E\,(\mathfrak{l}\,(G)/\mathfrak{l}\,(H)) = E\,(\mathfrak{g}/\mathfrak{h})$ are by definition the elements of the quotient algebra $\mathfrak{g}/\mathfrak{h}$, i.e. cosets $X + \mathfrak{h}$ of the algebra $\mathfrak{g}$ mod the ideal $\mathfrak{h}$. We show that the exponential mapping exp: $\mathfrak{g} \to G$ maps every such coset onto some coset aH of a local group G mod an invariant local subgroup $H = \exp \mathfrak{h}$. Indeed, as we already know, for any elements $X \in \mathfrak{g}$, $Y \in \mathfrak{h}$ sufficiently close to zero

$$\mathcal{H}\,(X,\ Y) = X + Y^*,$$

where $Y^* \in \mathfrak{h}$, with

$$Y^* = Y + \sum_{n>1} \mathcal{H}_n\,(X,\ Y),$$

from which it immediately follows that for any fixed X the mapping $Y \to Y^*$ is bijective (in some neighbourhood of zero). Hence the mapping

$$X + Y^* \mapsto \exp\,(X + Y^*) = \exp \mathcal{H}\,(X,\ Y) = \exp X \cdot \exp Y$$

maps every coset $X + \mathfrak{h}$ onto the coset $\exp X \cdot H$.

The constructed mapping of the manifold $E\,(\mathfrak{g}/\mathfrak{h})$ onto the manifold G/H is obviously a diffeomorphism in the identity. To complete the proof of Proposition 3 therefore it remains to show that it sends product to product. But this is obvious since for any elements $X_1,\ X_2 \in \mathfrak{g},\ Y_1,\ Y_2 \in \mathfrak{h}$ we have

$$\begin{aligned}(X_1 + Y_1^*)\cdot(X_2 + Y_2^*) &= \mathcal{H}\,(X_1 + Y_1^*,\ X_2 + Y_2^*) \\ &= \mathcal{H}\,(X_1,\ X_2) + Y^*,\end{aligned}$$

where $Y^* \in \mathfrak{h}$, and hence

$$\begin{aligned}(X_1 + Y_1^*)\cdot(X_2 + Y_2^*) &\mapsto \exp \mathcal{H}\,(X_1,\ X_2)\cdot \exp Y^* \\ &\in a_1H \cdot a_2H,\end{aligned}$$

where $a_1 = \exp X_1$, $a_2 = \exp X_2$. $\square$

We summarize the results obtained in the following theorem:

Theorem 1. *For every local Lie group G the Lie correspondence is a natural bijective correspondence between the lattice*

of all local subgroups of G and the lattice of all subalgebras of a Lie algebra $\mathfrak{g} = \mathfrak{l}(G)$.

Associated in this correspondence with invariant local subgroups are ideals of $\mathfrak{g}$ *and, conversely, associated with ideals are invariant local subgroups.*

The quotient algebra of a Lie algebra $\mathfrak{l}(G)$ *is a Lie algebra of every local factor group of G mod the corresponding ideal.* □

As we have already repeatedly stressed, all the results of the last lectures are related to *analytic* (i.e. class C^{ω}) local groups. It turns out that we have sustained no loss of generality. To give this statement an exact formulation we say, with some class of smoothness C^r (with $r \geqslant 2$) fixed, that local groups which are manifolds of the C^r class are *smooth local groups* and local groups of C^{ω} are *analytic local groups*. The following theorem then holds and shows that in terms of the theory of local Lie groups a restriction of the discussion to analytic local groups does not in fact decrease generality.

Theorem 2. *Every smooth local group is isomorphic (in the category of smooth local groups) to some analytic local group.*

The proof of this theorem is based on a property of the Lie functor, of interest in its own right, which is just to be discussed by us in the first place.

Let C and D be two categories and let F: $\mathsf{C} \to \mathsf{D}$ be a functor. For any two objects A, B of C the functor F gives some mapping

$$\mathrm{Mor}_{\mathsf{C}}(A, B) \to \mathrm{Mor}_{\mathsf{D}}(FA, FB)$$

of the set of all morphisms $A \to B$ of C into the set of all morphisms $FA \to FB$ of D. The functor F is said to be *completely univalent* if for any A and B that mapping is bijective, i.e. if for any morphism β: $FA \to FB$ there is one and only one morphism α: $A \to B$ for which $F\alpha = \beta$.

It is clear that if F is completely univalent, then the objects A and B of C are isomorphic if and only if so are the objects FA and FB of D. In the following proposition, by GR-LOC is meant the category of smooth local Lie groups.

Proposition 4. *The functor* GR-LOC $\to$ ALG$_f$-LIE *is completely univalent.*

In particular, local Lie groups are isomorphic if and only if so are their Lie algebras.

This proposition yields Theorem 2 at once. Indeed, let G be a smooth local group and $\mathfrak{g} = \mathfrak{l}(G)$ its Lie algebra. The functor E constructed in the preceding lecture associates with $\mathfrak{g}$ some analytic local group $E\mathfrak{g}$ whose Lie algebra $\mathfrak{l}(E\mathfrak{g})$ is isomorphic to $\mathfrak{g}$. Therefore that local group is isomorphic to G. $\square$

Notice that Proposition 4 is trivially true for analytic local groups, since *any quasi-invertible functor* $F\colon \mathsf{C} \to \mathsf{D}$ *is completely univalent*. Indeed, if $G\colon \mathsf{D} \to \mathsf{C}$ is a quasi-inverse functor, then for any morphism $\alpha\colon A \to B$ we have a commutative diagram

$$\begin{tikzcd} A \arrow[r, "\varepsilon_A"] \arrow[d] & GFA \arrow[d, "GF\alpha"] \\ B \arrow[r, "\varepsilon_B"] & GFB \end{tikzcd}$$

in which the horizontal arrows are isomorphisms. Therefore if $F\alpha = F\beta$, then

$$\alpha = \varepsilon_B^{-1} \circ GF\alpha \circ \varepsilon_A = \varepsilon_B^{-1} \circ GF\beta \circ \varepsilon_A = \beta.$$

Thus if for a morphism $\gamma\colon FA \to FB$ there is a morphism $\alpha\colon A \to B$ such that $F\alpha = \gamma$, then that morphism is unique. It is similarly proved that for a morphism $\alpha\colon GS \to GT$, where S, T are the objects of the category D, there can be only one morphism $\gamma\colon S \to T$ such that $G\gamma = \alpha$. On the other hand, for any morphism $\gamma\colon FA \to FB$ the morphism $\alpha = \varepsilon_B^{-1} \circ G\gamma \circ \varepsilon_A$ has the property that $GF\alpha = \varepsilon_B \circ \alpha \circ \varepsilon_A^{-1} = G\gamma$. Therefore $F\alpha = \gamma$. $\square$

The proof of Proposition 4 is based on the theory of exact differential equations (Pfaffian differential equations). We begin by presenting this theory in invariant form using no coordinates.

Let P and Q be two smooth manifolds.

Definition 6. *A Pfaffian system* from P to Q is the function

$$f\colon (p, q) \mapsto f(p, q)$$

which associates with every point $(p, q) \in P \times Q$ some linear mapping

$$f(p, q)\colon \mathsf{T}_p(P) \to \mathsf{T}_q(Q)$$

which is smoothly dependent on p and q.

If $x^1, \ldots, x^n$ and $y^1, \ldots, y^m$ are local coordinates in manifolds P and Q respectively, then in the associated coordinates on vector spaces $\mathsf{T}_p(P)$ and $\mathsf{T}_q(Q)$ the mapping $f(p, q)$ will be given by an $n \times m$ matrix whose elements are functions of $x^1, \ldots, x^n$ and $y^1, \ldots, y^m$. The requirement that $f(p, q)$ should be smoothly dependent on p and q means that the functions are smooth.

Remark 1. In more invariant terms the concept of Pfaffian system is defined through that of *induced fibering*. We shall not recall that concept (we shall no longer need it anywhere) but only remark that a Pfaffian system in the sense of Definition 6 is nothing but the mapping over $P \times Q$ of the fibering induced from the tangent fibering $\mathsf{T}(P)$ by the projection $P \times Q \to P$ into the fibering induced from the tangent fibering $\mathsf{T}(Q)$ by the projection $P \times Q \to Q$. This approach allows one to avoid explaining the requirement that mappings $f(p, q)$ should be smoothly dependent on p and q.

Definition 7. An *integral* of a Pfaffian system f on an open set $U \subset P$ is a mapping $\varphi\colon U \to Q$ such that

$$f(u, \varphi x) = (d\varphi)_u$$

for any point $u \in U$. The Pfaffian system f is said to be *integrable* if for every point $(p_0, q_0) \in P \times Q$ there is an integral $\varphi\colon U \to Q$ of f defined on some neighbourhood U of the point p_0 in the manifold P such that $\varphi(p_0) = q_0$.

Lemma 1. *Any two integrals $\varphi\colon U \to Q$ and $\varphi'\colon U' \to Q$ defined on U and U' of p_0 and such that $\varphi(p_0) = \varphi'(p_0)$ coincide on some neighbourhood of p_0.*

We shall prove that Lemma below.

To obtain convenient conditions for the integrability of the Pfaffian system (and to prove Lemma 1 at the same time) it is appropriate to somewhat generalize the problem.

Let M be an arbitrary smooth manifold and $\pi\colon \mathsf{T}(M) \to M$ its tangent fibering.

Definition 8. A vector bundle $\pi_1: E \to M$ is said to be a *subfibering* of a tangent fibering (or bundle) $\pi: \mathsf{T}(M) \to M$ if $E \subset \mathsf{T}(M)$, the embedding $E \to \mathsf{T}(M)$ is smooth and $\pi_1 = \pi|_E$. The subfibering is uniquely defined by giving a manifold E, and as a rule we shall identify it with E. The fibre $\pi_1^{-1}(a)$ of the fibering E over a point $a \in M$ will be denoted by E_a. It is the subspace $\mathsf{T}_a(M) \cap E$ of the tangent space $\mathsf{T}_a(M)$ whose dimension is the same for all a and will be denoted by m.

For every open set $U \subset M$ a vector bundle $\pi_1^{-1}(U) \to U$ is defined which has the same fibres as the fibering E. It is a subfibering of the tangent bundle $\mathsf{T}(U) \to U$. We shall denote that subfibering by $E|_U$ and call it a *restriction* of the subfibering E to U.

By this definition $\mathsf{T}(M)|_U = \mathsf{T}(U)$.

Let W be an m-dimensional manifold and w_0 its point. As a rule W will be assumed to be a neighbourhood of w_0 in some manifold ($\mathbb{R}^m$, for example), but in principle W may be arbitrary.

Definition 9. A smooth mapping $\Phi: W \to M$ is said to be *integral with respect to a subfibering* $E \subset \mathsf{T}(M)$ if at any point $w \in W$ its differential

$$(d\Phi)_w: \mathsf{T}_w(W) \to \mathsf{T}_a(M), \quad a = \Phi w$$

is a monomorphism onto a fibre E_a of the subfibering E.

In accordance with the generally accepted set-theoretic notation we shall write $\Phi: (W, w_0) \to (M, a_0)$ if $a_0 = \Phi w_0$.

Definition 10. A subfibering E of a tangent bundle $\mathsf{T}(M)$ is said to be *integrable* if for any point $a_0 \in M$ there is a mapping $\Phi: (W, w_0) \to (M, a_0)$ which is integral with respect to E.

Lemma 2. *If a subfibering E is integrable, then for any point $a_0 \in M$ and any E-integral mappings $\Phi: (W, w_0) \to (M, a_0)$ and $\Phi': (W', w_0) \to (M, a_0)$ there are neighbourhoods V and V' of w_0 and w_0' and a diffeomorphism $\beta: V' \to V$ in manifolds W and W' such that $\Phi' = \Phi \circ \beta$ on V'.*

We shall prove this lemma later on.

Let f be a Pfaffian system from P to Q and let $M = P \times Q$. For any point $a = (p, q) \in M$, we shall consider a *graph* of the mapping $f(p, q): \mathsf{T}_p(P) \to \mathsf{T}_p(Q)$, i.e. a subset E_a

of the direct sum

$$\mathsf{T}_a(M) = \mathsf{T}_p(P) \oplus \mathsf{T}_q(Q)$$

consisting of vectors (A, B), $A \in \mathsf{T}_p(P)$, $B \in \mathsf{T}_q(Q)$ such that

$$B = f(p, q)\, A.$$

Since the mapping $f(p, q)$ is linear, that subset is a subspace.

We put

$$E = \bigcup_{a \in M} E_a.$$

The set E is a subset in $\mathsf{T}(M)$ and a restriction $\pi_2\colon E \to M$ to E of the projection $\pi\colon \mathsf{T}(M) \to M$ has the property such that $\pi_1^{-1}(a) = E_a$ for any point $a \in M$.

If $(U \times V, h \times k)$ is a chart on M which is the product of charts (U, k) and (V, k) on P and Q respectively and if

$$W = \pi_1^{-1}(U \times V) = \bigcup_{a \in U \times V} E_a,$$

the mapping

$$W \to (U \times V) \times \mathbb{R}^m, \qquad m = \dim P$$

defined by the formula

$$(A, B) \mapsto (\pi(A, B), \dot{h}A),$$

where $\dot{h}\colon \mathsf{T}_p(P) \to \mathbb{R}^m$, $p = \pi A$ is a chart corresponding to a chart h, will obviously be a bijective mapping. The inverse mapping H sends a point (a, x), where $a = (p, q) \in U \times V$ and $x \in \mathbb{R}^m$, to a vector $(h^{-1}x, f(p, q)\, \dot{h}^{-1}x)$ and has therefore the property that for every point $a \in U \times V$ the mapping $x \mapsto H(a, x)$ is an isomorphism of vector space $\mathbb{R}^m$ onto vector space E_a.

If (U', h') is another chart on P and

$$H'\colon (U' \times V) \times \mathbb{R}^m \to W' = \bigcup_{a \in U' \times V} E_a$$

is the corresponding mapping, then (with $U \cap U' \neq \varnothing$) for any point $a \in (U \times V) \cap (U' \times V)$ the composition of the mapping $x \mapsto H(a, x)$ and the mapping inverse to the mapping $x \mapsto H'(a, x)$ will obviously coincide with the

mapping $\dot{h}' \circ \dot{h}^{-1}: \mathbb{R}^m \to \mathbb{R}^m$ and will hence smoothly depend on a.

This means that (E, π_1, M) is a vector bundle. In addition, it is clear that the embedding $E \to \mathsf{T}(M)$ is smooth and therefore (since by construction $\pi_1 = \pi|_E$) that mapping is a subfibering of the tangent bundle $\mathsf{T}(M)$.

Definition 11. The subfibering constructed is called a *graph* of a Pfaffian system f.

It is obvious that a mapping $\varphi: U \to Q$ is an integral of the Pfaffian system f if and only if the mapping $\Phi: U \to P \times Q$ defined by the formula

$$\Phi u = (u, \varphi u), \qquad u \in U \tag{4}$$

is integral with respect to the graph E of f. On the other hand, if $\Psi: W \to P \times Q$ is a mapping integral with respect to the graph E and $\Psi w = (\alpha w, \psi w)$, where $\alpha: W \to P$, $\psi: W \to Q$, then it is easily seen that for any point $w_0 \in W$ the differential $(d\alpha)_{w_0}$ of a mapping α will be an isomorphism and that hence, possibly after going from W to a smaller neighbourhood of the point w_0, the mapping α will itself be a diffeomorphism of the manifold W onto some neighbourhood U of the point $u_0 = \alpha w_0$. Then the mapping $\Phi = \Psi \circ \alpha^{-1}: U \to P \times Q$, while continuing to be integral with respect to the subfibering E, will be given by formula (4) (with $\varphi = \psi \circ \alpha^{-1}$) and will therefore define an integral φ of the Pfaffian system f. This proves that *the Pfaffian system from P and Q is integrable if and only if its graph is an integrable subfibering of the tangent bundle of the manifold $P \times Q$.*

In addition, we can now prove (assuming Lemma 2 established) Lemma 1.

Proof of Lemma 1. Let $\varphi: (U, u_0) \to (Q, q_0)$ and $\varphi': (U', u_0) \to (Q, q_0)$ be two integrals of a Pfaffian system f which coincide at the point $u_0 \in U \cap U'$ and let $\Phi: u \mapsto (u, \varphi u)$ and $\Phi': u \mapsto (u, \varphi' u)$ be the corresponding mappings (4) integral with respect to the graph E of that system. By Lemma 2 there are neighbourhoods V and V' of u_0 and a diffeomorphism $\beta: V' \to V$ such that $\Phi' = \Phi \circ \beta$ onto V'. Projecting onto U we see, in particular, that $\beta u = u$ for any point $u \in V'$, i.e. that $V' = V$ and $\beta = \mathrm{id}$. But then $\varphi' = \varphi' \circ \beta = \varphi'$ onto $V' = V$, which proves Lemma 1. □

Suppose again that E is a subfibering of the bundle $\mathsf{T}(M)$. We shall say that a vector field $X \in \mathfrak{a}(M)$ *is in* E if $X_a \in E_a$ for any point $a \in M$. Clearly, all such fields form a submodule of the $\mathscr{F}(M)$-module $\mathfrak{a}(M)$. We shall denote that submodule by $\mathfrak{a}(E)$.

If the fibering E is trivial (isomorphic to the fibering $M \times \mathbb{R}^n \to M$), then there are vector fields $X_1, \ldots, X_m$ on M such that for any point $a \in M$ vectors $(X_1)_a, \ldots, (X_m)_a$ form a basis of the space E_a and hence $X_1, \ldots, X_m$ form a basis of the $\mathscr{F}(M)$-module $\mathfrak{a}(E)$. i.e. the module is free. It follows from the local triviality of E that for *any subfibering E of the tangent bundle $\mathsf{T}(M)$ there is an open covering $\{U\}$ of the manifold M, such that for every element U of that covering the $\mathscr{F}(U)$-module $\mathfrak{a}(E|_U)$ is free.*

Definition 12. A subfibering E is said to be *involutory* if the submodule $\mathfrak{a}(E)$ is a subalgebra of a Lie algebra $\mathfrak{a}(M)$, i.e. if $[X, Y] \in \mathfrak{a}(E)$ for any fields $[X, Y] \in \mathfrak{a}(E)$.

Below we shall encounter a situation where the submodule $\mathfrak{a}(E)$ is generated by some (finite-dimensional) subalgebra $\mathfrak{g}$ of a Lie algebra $\mathfrak{a}(M)$, i.e. where any element of it is a linear combination with coefficient from $\mathscr{F}(M)$ of fields in $\mathfrak{g}$ (according to the standard notation of module theory such a submodule will be denoted by $\mathscr{F}(M)\,\mathfrak{g}$). It is easily seen that in this case the condition of involutedness is satisfied, i.e. *any submodule generated by a subalgebra is itself a subalgebra.* Indeed, it is obviously sufficient to show that for any fields $X, Y \in \mathfrak{g}$ and any function $f \in \mathscr{F}(M)$ the field $[fX, Y]$ is in $\mathscr{F}(M)\,\mathfrak{g}$. But since Y is a differentiation, we have $Y \circ fX = Yf \cdot X + f \cdot Y \circ X$ and therefore

$$\begin{aligned}[fX, Y] &= fX \circ Y - Y \circ fX = f\cdot(X \circ Y - Y \circ X) - Yf\cdot X \\ &= f\cdot[X, Y] - Yf\cdot X \in \mathscr{F}(M)\,\mathfrak{g},\end{aligned}$$

since $[X, Y] \in \mathfrak{g}$ and $Yf \in \mathscr{F}(M)$. □

Proposition 5 (Frobenius theorem). *A subfibering E is integrable if and only if it is involutory.*

Before proving the proposition we apply it to the proof of Proposition 4.

Proof of Proposition 4. Let G and H be two smooth local Lie groups and $f: \mathfrak{g} \to \mathfrak{h}$ an arbitrary homomorphism of the Lie algebra $\mathfrak{g} = \mathfrak{l}(G)$ into the Lie algebra $\mathfrak{h} = \mathfrak{l}(H)$. It is

necessary to show that there is a homomorphism $\varphi\colon G \to H$ of G into H for which $\mathfrak{l}(\varphi) = f$ and that the homomorphism is unique.

To this end, interpreting f as a mapping $\mathsf{T}_e(G) \to \mathsf{T}_e(H)$ we can define for any two elements $a \in G$ and $b \in H$ a linear mapping $f(a, b)\colon \mathsf{T}_a(G) \to \mathsf{T}_b(H)$ by putting

$$f_{(a,\, b)} = (dL_b)_e \circ f \circ (dL_a)_e^{-1}, \tag{5}$$

where, as ever, L_a and L_b are the left shifts. Clearly, mappings $f(a, b)$ smoothly depend on a and b, i.e. form some Pfaffian system from G to H.

For any homomorphism $\varphi\colon G \to H$ of local Lie groups and any element $a \in G$ a relation $\varphi \circ L_a = L_{\varphi a} \circ \varphi$ holds (signifying that $\varphi(ax) = \varphi a \varphi x$), i.e. a relation $\varphi = L_{\varphi a} \circ \varphi \circ L_a^{-1}$. Therefore

$$(d\varphi)_a = (dL_{\varphi a})_e \circ (d\varphi)_e \circ (dL_a)_e^{-1},$$

from which it follows that if $f = \mathfrak{l}(\varphi)$, i.e. $f = (d\varphi)_e$, then

$$(d\varphi)_a = f(a, \varphi a),$$

i.e. φ is an integral of the Pfaffian system (5), which has the property that $\varphi e = e$.

Suppose for the Pfaffian system (5) there is an integral φ defined on some neighbourhood of the identity e of G and such that $\varphi e = e$. Since equivalent local groups are not distinguished, we may assume without loss of generality that φ is defined on the entire local group G.

For any fixed point $a \in G$ the mapping $\varphi \circ L_a\colon x \mapsto \varphi(ax)$ defined on some neighbourhood of e satisfies the relation

$$\begin{aligned} d(\varphi \circ L_a)_x &= (d\varphi)_{ax} \circ (dL_a)_x \\ &= (dL_{\varphi(ax)})_e \circ f \circ (dL_{ax})_e^{-1} \circ (dL_a)_x \\ &= (dL_{\varphi(ax)})_e \circ f \circ (dL_x)_e^{-1} = f(x, \varphi(ax)), \end{aligned}$$

i.e. it is an integral of (5). Similarly, since

$$\begin{aligned} (dL_{\varphi(a)} \circ \varphi)_x &= (dL_{\varphi(a)})_{\varphi x} \circ (d\varphi)_x \\ &= (dL_{\varphi(a)})_{\varphi x} \circ (dL_{\varphi x})_e \circ f \circ (dL_x)_e^{-1} \\ &= (dL_{\varphi a \cdot \varphi x})_e \circ f \circ (dL_x)_e^{-1} \\ &= f(x, \varphi a \varphi x), \end{aligned}$$

the mapping $L_{\varphi a} \circ \varphi\colon x \mapsto \varphi a \varphi x$ is also an integral of (5). As both integrals assume for $x = e$ the same value φa, by Lemma 1 they coincide in some neighbourhood of e. Thus, in that neighbourhood $\varphi(ax) = \varphi a \varphi x$ and hence φ is a homomorphism of G into H. Since

$$(d\varphi)_e = (dL_e)_e \circ f \circ (dL_e)_e^{-1} = f,$$

that homomorphism induces the given homomorphism f of Lie algebras.

This proves that homomorphisms $\varphi\colon G \to H$ of local Lie groups, that induce the given homomorphism $f\colon \mathfrak{g} \to \mathfrak{h}$ of Lie algebras are precisely the integrals of system (5) for which $\varphi e = e$. To prove Proposition 4 it then suffices to establish that system (5) is integrable, i.e. that so is the subfibering E of the tangent bundle $\mathsf{T}(G \times H)$ which is the graph of that system.

The fibre of that graph over the point $(e, e) \in G \times H$ is obviously a graph $\mathfrak{f}$ of f, i.e. a subspace of the space $\mathsf{T}_e(G \times H) = \mathsf{T}_e(G) \times \mathsf{T}_e(H)$ made up of pairs of the form (A, fA), where $A \in \mathsf{T}_e(G)$. But over an arbitrary point $(a, b) \in G \times H$ the fibre of the graph is obtained by acting upon f by a linear operator $dL_{(a, b)} = dL_a \times dL_b$.

If therefore we consider on $G \times H$ left-invariant vector fields $X_1, \ldots, X_m$ whose values $X_1(e, e), \ldots, X_m(e, e)$ at the point (e, e) form a basis of the subspace $\mathfrak{f}$, then their values $X_1(a, b), \ldots, X_m(a, b)$ at any point $(a, b) \in G \times H$ will form a basis of the fibre of the graph E over (a, b). This means that the *fields* $X_1, \ldots, X_m$ *form a basis of the* $\mathcal{F}(G \times H)$*-module* $\mathfrak{a}(E)$ (so that this module is free).

To restate this in more invariant terms, we should notice that the subspace $\mathfrak{f}$ of the Lie algebra $\mathfrak{l}(G \times H) \subset \mathfrak{a}(G \times H)$, being the graph of a homomorphism of Lie algebras, is a subalgebra of that algebra and hence of the entire Lie algebra $\mathfrak{a}(G \times H)$. If $\mathfrak{l}(G \times H)$ is interpreted as the algebra of left-invariant vector fields, the basis of the subalgebra $\mathfrak{f}$ will form exactly the fields $X_1, \ldots, X_m$. Therefore the submodule of the $\mathcal{F}(G \times H)$-module $\mathfrak{a}(G \times H)$, which has the basis $X_1, \ldots, X_m$, is precisely the submodule $\mathcal{F}(G \times H)\mathfrak{f}$ generated by the subalgebra $\mathfrak{f}$. But it was noticed above that a submodule generated by a subalgebra is itself a subalgebra. Thus the submodule $\mathfrak{a}(E)$ is a subalge-

bra of the algebra $\mathfrak{a}(G \times H)$, so that the subfibering E is involutory. Hence, by Proposition 5, it is integrable. □

It now remains to merely prove Proposition 5 (and Lemma 2). The condition of necessity of this proposition is proved without difficulty:

Proposition 6. *Any integrable subfibering E is involutory.*

Proof. Let $a_0 \in M$ and $\Phi: (W, w_0) \to (M, a_0)$ be a mapping integral with respect to E. Since at any point $w \in W$ the mapping $(d\Phi)_w : \mathsf{T}_w(W) \to \mathsf{T}_{\Phi w}(M)$ is monomorphic, for any vector field $X \in \mathfrak{a}(E)$ there is a unique field X^Φ on W that satisfies the relation

$$X_{\Phi w} = (d\Phi)_w (X^\Phi_w),$$

i.e. a field Φ-connected with the field X. For any two fields $X, Y \in \mathfrak{a}(E)$ the fields $[X, Y]$ and $[X^\Phi, Y^\Phi]$ are also Φ-connected, i.e. for them

$$[X, Y]_{\Phi w} = (d\Phi)_w [X^\Phi, Y^\Phi]_w.$$

Thus $[X, Y]_{\Phi w} \in \operatorname{Im}(d\Phi)_w = E_{\Phi w}$. In particular, $[X, Y]_{a_0} \in E_{a_0}$. Since the point $a_0 \in M$ is arbitrary, this proves that $[X, Y] \in \mathfrak{a}(E)$. Consequently, the subfibering E is involutory. □

The converse is more delicate to prove.

Definition 13. A subfibering E of the tangent bundle $\mathsf{T}(M)$ is said to be *completely integrable* if the manifold M has an atlas made up of charts $(U, x^1, \ldots, x^n)$ such that for any point $a \in U$ the first m vectors $\left(\frac{\partial}{\partial x^1}\right)_a, \ldots, \left(\frac{\partial}{\partial x^m}\right)_a$ of the basis $\left(\frac{\partial}{\partial x^1}\right)_a, \ldots, \left(\frac{\partial}{\partial x^n}\right)_a$ of the space $\mathsf{T}_a(M)$ form a basis of the spase E_a, i.e. in other words such that the vector fields $\frac{\partial}{\partial x^1}, \ldots, \frac{\partial}{\partial x^m}$ on U form a basis of the $\mathcal{F}(U)$-module $\mathfrak{a}(E|_U)$.

It is easy to see that *any completely integrable subfibering is integrable*. Indeed let $a_0 \in M$ and $a_0 \in U$, where $(U, h) = (U, x^1, \ldots, x^n)$ is a chart from an atlas specified by Definition 13. Suppose next that $\mathcal{L}^m$ is a plane $x^{m+1} = x^{m+1}(a_0), \ldots, x^n = x^n(a_0)$ of the space $\mathbb{R}^n$ and that

W is the intersection $\mathscr{L}^m \cap h(U)$ (containing obviously the point $w_0 = h(a_0)$). Finally let $\Phi\colon W \to M$ be a restriction to W of the inverse diffeomorphism $h^{-1}\colon h(U) \to U$ (considered as a mapping in M). The differential $(d\Phi)_w$ of the mapping Φ at a point $w \in W$ sends the standard basis of the space $\mathsf{T}_w(W) = \mathbb{R}^m$ to vectors $\left(\frac{\partial}{\partial x^1}\right)_a, \ldots, \left(\frac{\partial}{\partial x^m}\right)_a$, where $a = \Phi w$, and is therefore a monomorphism onto the space E_a.

Thus the mapping $\Phi\colon (W, w_0) \to (M, a_0)$ is a mapping integral with respect to E. Since $a_0 \in M$ is an arbitrary point, this precisely means that the subfibering E is integrable. $\square$

Moreover, it can be shown similarly that *any completely integrable subfibering E has the property stated in Lemma* 2, i.e. for any two E-integral mappings $\Phi\colon (W, w_0) \to (M, a_0)$ and $\Phi'\colon (W', w_0') \to (M, a_0)$ there are neighbourhoods V and V' of the points w_0 and w_0' and a diffeomorphism $\beta\colon V' \to V$ in W and W', such that $\Phi' = \Phi \circ \beta$ onto V'. Indeed, we may assume without loss of generality that Φ' is the above-constructed mapping from the chart $(U, x^1, \ldots, x^n)$ and that the manifold W is an open subset of the space $\mathbb{R}^m$. Then for any point $w = (w^1, \ldots, w^m) \in W$ the vectors $(d\Phi)_w\left(\frac{\partial}{\partial w^1}\right), \ldots, (d\Phi)_w\left(\frac{\partial}{\partial w^m}\right)$ will form a basis of E_a, $a = \Phi w$, and will therefore be linearly expressed in terms of vectors $\left(\frac{\partial}{\partial x^1}\right)_a, \ldots, \left(\frac{\partial}{\partial x^m}\right)_a$. On the other hand, if $x^1(w), \ldots, x^n(w)$ are the functions giving the mapping Φ, then

$$(d\Phi)_w\left(\frac{\partial}{\partial w^i}\right) = \left(\frac{\partial x^j}{\partial w^i}\right)_w \cdot \left(\frac{\partial}{\partial x^j}\right)_a, \quad i = 1, \ldots, m,$$

according to the general rule defining in coordinates the action of the differential of a smooth mapping. Hence $\frac{\partial x^j}{\partial w^i} = 0$ on W for any $i = 1, \ldots, m$ and any $j = m + 1, \ldots, n$, and therefore $x^j(w) = \text{const}$ (more precisely $x^j(w) = x^j(a_0)$) for $j = m + 1, \ldots, n$. This means that the composition $\beta = h \circ \Phi$ of a mapping Φ and a coordinate diffeomorphism h is a mapping $W \to W'$. Since β is obvious-

ly an étale mapping, w_0 has a neighbourhood V on which that mapping is a diffeomorphism onto some neighbourhood V' of w_0'. To complete the proof it remains to notice that $\Phi = h^{-1} \circ (h \circ \Phi) = \Phi \circ \beta$ onto V. $\square$

By virtue of these remarks, to prove Lemma 2 and the remainder of Proposition 5 it is sufficient to establish the following proposition:

Proposition 7. *Any involutory subfibering E of the tangent bundle $\mathsf{T}(M)$ is completely integrable.*

Proof. Let a_0 be a point of a manifold M and let $(U, h) = (U, x^1, \ldots, x^n)$ be some chart of M at that point. On choosing a smaller neighbourhood, if necessary, we may assume that the $\mathcal{F}(U)$-module $\mathfrak{a}(E|_U)$ is free, i.e. has a basis consisting of m vector fields $X_1, \ldots, X_m$. To simplify the formulas, it may also be assumed that $x^1(a_0) = 0, \ldots, x^n(a_0) = 0$.

Suppose first that $m = 1$. Setting $X = X_1$, consider the components $X^1 = Xx^1, \ldots, X^n = Xx^n$ of the vector field X in coordinates $x^1, \ldots, x^n$. Since $X \neq 0$ in U, it may be assumed without loss of generality that $X^n \neq 0$ in U (it suffices, if necessary, to rewrite the coordinates and make U smaller).

As we know, for any point $u \in U$ there is an integral curve $\varphi_u : I_u \to M$ of X defined on some interval I_u of the axis $\mathbb{R}$, containing the point 0, and such that $\varphi_u(0) = u$. It may be assumed (again making U smaller, if necessary) that I_u is independent of u (I is the same for all u).

Now consider in the space $\mathbb{R}^n = \mathbb{R}^{n-1} \times \mathbb{R}$ an open set $W \times I$, where W is the set of all points $\boldsymbol{w} = (w_1, \ldots w^{n-1}) \in \mathbb{R}^{n-1}$ for which $(\boldsymbol{w}, 0) \in h(U)$, and a mapping

$$\Phi\colon W \times I \to M$$

of that set in the manifold M, that is defined by the formula

$$\Phi(w, t) = \varphi_u(t), \quad \text{where } u = h^{-1}(w, 0).$$

In coordinates $w^1, \ldots, w^{n-1}, w^n = t$ and $x^1, \ldots, x^n$, that mapping can be written using functions $x^1(\boldsymbol{w}, t), \ldots, x^n(\boldsymbol{w}, t)$ such that

$$\text{(6)} \qquad \frac{dx^i(\boldsymbol{w}, t)}{dt} = X^i(x^1(\boldsymbol{w}, t), \ldots, x^n(\boldsymbol{w}, t)), \quad i = 1, \ldots, n,$$

and

$$x^1(w, 0) = w^1, \ldots, x^{n-1}(w, 0) = w^{n-1}, x^n(w, 0) = 0$$

are identical for w. In particular, we see that

$$\left(\frac{\partial x^i}{\partial w^j}\right)_{t=0} = \delta^i_j \quad \text{and} \quad \left(\frac{\partial x^n}{\partial t}\right)_{t=0} = 0.$$

This means together with formulas (6) that at any point of the form $(w, 0)$ and, in particular, at the point $(\mathbf{0}, 0)$ the matrix of the differential of Φ is, in the coordinates $w^1, \ldots, w^{n-1}, w^n = t$ and $x^1, \ldots, x^n$, of the form

$$\begin{pmatrix} 1 & & X^1 \\ \cdot & 0 & \cdot \\ & \cdot & \cdot \\ 0 & \cdot & \cdot \\ & 1 & X^{n-1} \\ 0\ldots & 0 & X^n \end{pmatrix}$$

and is therefore (since $X^n \neq 0$) nonsingular. Hence Φ is étale at the point $\mathbf{0} = (\mathbf{0}, 0) \in W \times I$ and may therefore be assumed without loss of generality to be a diffeomorphism of the set $W \times I$ onto the neighbourhood U. The inverse diffeomorphism Φ^{-1} defines on U coordinates $w^1, \ldots, w^{n-1}, w^n$ that obviously have the property that $\frac{\partial}{\partial w^n} = X$ on U.

There are thus coordinates $w^1, \ldots, w^n$ in some neighbourhood of the point a_0 such that the field $\frac{\partial}{\partial w^n}$ generates a submodule $\mathfrak{a}(E|_U)$. Since a_0 was chosen arbitrarily, this proves that E is a completely integrable subfibering.

This completes the proof of Proposition 6 for $m = 1$. (Notice that for $m = 1$ the condition of involutedness is directly satisfied.)

Now let $m > 1$. Proceeding by induction, assume that Proposition 6 has already been proved for subfiberings having fibres of dimension $m - 1$ and consider an involutory subfibering E with fibres of dimension m.

Lemma 3. *On a manifold M, there is a chart $(U, x^1, \ldots, x^n)$ with $a_0 \in U$ and a basis $X_1, \ldots, X_m$ of a module $\mathfrak{a}(E|_U)$*

such that

(a) $$X_m x^1 = \ldots = X_m x^{n-1} = 0,$$
$$X_m x^n = 1, \quad i.e. \quad X_m = \frac{\partial}{\partial x^n};$$

(b) $X_1 x^n = \ldots = X_{m-1} x^n = 0$, *i.e. the fields* $X_1, \ldots, X_{m-1}$ *can be expressed only in terms of the field* $\frac{\partial}{\partial x^1}, \ldots, \frac{\partial}{\partial x^{n-1}}$;

(c) *with* $x^n = 0$, *the functions* $X_1 x^j, \ldots, X_{m-1} x^j$, $m \leqslant j \leqslant n$, *of* $x^1, \ldots, x^{n-1}$ *are identically zero.*

Proof. First suppose $(U, x_1, \ldots, x_n)$ is a chart (with $a_0 \in U$) such that the module $\mathfrak{a}(E|_U)$ is free and let $X_1, \ldots, X_m$ be a basis of $\mathfrak{a}(E|_U)$. The vector field X_m generates a subfibering for which $m = 1$; applying to that subfibering that part of Proposition 7 which was already proved we find a chart (denote it again by $(U, x^1, \ldots, x^n)$) that satisfies condition (a).

To satisfy condition (b) we replace the fields $X_1, \ldots, X_{m-1}$ by the fields

$$X_1 - (X_1 x^n) X_m, \ldots, X_{m-1} - (X_{m-1} x^n) X_m.$$

It is clear that taken together with X_m they also form a basis of $\mathfrak{a}(E|_U)$ and (again denoted by $X_1, \ldots, X_{m-1}$) satisfy condition (b).

Condition (c) is much more difficult to satisfy.

Let $W \subset \mathbb{R}^{n-1}$ be the same set as in the first part of the proof ($w \in W$ if and only if $(w, 0) \in h(U)$). Identifying W with $W \times 0$, consider a restriction $\varphi: W \to U$ to W of the diffeomorphism h^{-1} inverse to a coordinate diffeomorphism $h: U \to h(U) \subset \mathbb{R}^n$. For any point $w \in W$ the differential $(d\varphi)_w$ of the mapping φ is a monomorphic mapping of the vector space $\mathbf{T}_w(W) = \mathbb{R}^{n-1}$ onto a subspace of the vector space $\mathbf{T}_a(M)$, $a = \varphi(w)$ spann ed by the vectors $\left(\frac{\partial}{\partial x^1}\right)_a, \ldots, \left(\frac{\partial}{\partial x^{n-1}}\right)_a$. On W therefore there are uniquely defined vector fields

$$Y_1, \ldots, Y_{m-1}$$

φ-connected with the fields $X_1, \ldots, X_{m-1}$ (for which we assume conditions (a) and (b) to be satisfied). Denoting

the span of vectors $(Y_1)_w, \ldots, (Y_{m-1})_w$ for every point $w \in W$ by $(\varphi^*E)_w$, we obtain over W the subfibering φ^*E of the tangent bundle $\mathsf{T}(W)$ which has the property that the morphism $\mathsf{T}(\varphi)\colon \mathsf{T}(W) \to \mathsf{T}(M)$ of vector bundles maps it into the subfibering E.

By construction the vector fields $Y_1, \ldots, Y_{m-1}$ form a basis of the $\mathscr{F}(W)$-module $\mathfrak{a}(\varphi^*E)$. Since for any point $w \in W$

$$(d\varphi)_w [Y_i, Y_j]_w = [X_i, X_j]_{\varphi(w)} \in E_{\varphi(w)},$$

we have $[Y_i, Y_j]_w \in (\varphi^*E)_w$ and hence $[Y_i, Y_j] \in \mathfrak{a}(\varphi^*E)$. This means that φ^*E is an involutory subfibering.

Consequently, by induction on W, there are (possibly after making U, and hence W smaller) (curvilinear) coordinates $w^1, \ldots, w^{n-1}$ such that the vector fields $\frac{\partial}{\partial w^1}, \ldots, \frac{\partial}{\partial w^{n-1}}$ generate a submodule $\mathfrak{a}(\varphi^*F)$. Since the fields $Y_1, \ldots, Y_{m-1}$ have the same property, it follows that the fields $Y_1, \ldots, Y_{m-1}$ can be expressed only in terms of $\frac{\partial}{\partial w^1}, \ldots, \frac{\partial}{\partial w^{m-1}}$ and therefore their components $Y_1 w^j, \ldots, Y_{m-1} w^j$ in the basis $\frac{\partial}{\partial w^1}, \ldots, \frac{\partial}{\partial w^{n-1}}$ are zero for $m \leqslant j \leqslant n$.

It may be assumed without loss of generality that $h(U) = W \times I$, where I is some interval of the axis $\mathbb{R}$, and therefore on putting $h(u) = (w, x^n)$ we may associate with any point $u \in U$ as its local coordinates the coordinates $w^1, \ldots, w^{n-1}$ of a point $w \in W$ and the coordinate $x^n \in I$. In other words we introduce in U new local coordinates $y^1 = w^1, \ldots, y^{n-1} = w^{n-1}, y^n = x^n$ by taking as coordinate diffeomorphism $U \to h(U)$ the diffeomorphism inverse to the diffeomorphism $(\varphi \circ k) \times \mathrm{id}$, where $k\colon W \to W'$ is a diffeomorphism giving in W local coordinates $w^1, \ldots, w^{n-1}$. The coordinates $y^1, \ldots, y^n$ have the property such that $y^n = x^n$ and $y^1, \ldots, y^{n-1}$ are independent of x^n, so that

$$\frac{\partial y^1}{\partial x^n} = 0, \quad \ldots, \quad \frac{\partial y^{n-1}}{\partial x^n} = 0$$

and

$$\frac{\partial y^n}{\partial x^1} = 0, \quad \ldots, \quad \frac{\partial y^n}{\partial x^{n-1}} = 0, \quad \frac{\partial y^n}{\partial x^n} = 1.$$

Therefore the components $Xy^1, \ldots, Xy^n$ of an arbitrary vector field X relative to the coordinates $y^1, \ldots, y^n$ can be expressed in terms of its components $X^1 = Xx^1, \ldots, X^n = Xx^n$ relative to the coordinates $x^1, \ldots, x^n$ by the formulas

$$Xy^i = X^j \frac{\partial y^i}{\partial x^j}$$

$$= \begin{cases} X^1 \dfrac{\partial y^i}{\partial x^1} + \ldots + X^{n-1} \dfrac{\partial y^i}{\partial x^{n-1}}, & \text{if } i = 1, \ \ldots, \ n-1, \\ X^n, & \text{if } i = n. \end{cases}$$

In particular, for the field $X = X_m$ (for which under the hypothesis $X^1 = 0, \ldots, X^{n-1} = 0$, $X^n = 1$) we obtain that $X_m y^1 = 0, \ldots, X_m y^{n-1} = 0$, $X_m y^n = 1$, i.e. that $X_m = \frac{\partial}{\partial y^n}$. But for the fields $X_1, \ldots, X_{m-1}$ it follows that $X_1 y^n = \ldots = X_{m-1} y^n = 0$, i.e. that these fields can be linearly expressed only in terms of the field $\frac{\partial}{\partial y^1}, \ldots \frac{\partial}{\partial y^{n-1}}$. This means that in the chart $(U, y^1, \ldots, y^n)$ conditions (a) and (b) still hold.

In addition, for $y^n = 0$, i.e. at a point of the form $u = (\varphi(w), w \in W$, for a value $(X_i)_u$ of a vector field X_i, $i = 1, \ldots, n-1$ we have a formula

$$(X_i)_u = (d\varphi)_w Y_i$$

which expresses the φ-connectedness of the fields X_i and Y_i. As applied to functions $X_i y^j$ that formula shows that the value

$$(X_i y^j)(u) = (X_i)_u x^j$$

of $X_i y^j$ at $u \in U$ with $y^n(u) = 0$ is equal to that of $Y_i y^j$ at the point w. Since $Y_i y^j = 0$ for $m \leqslant j \leqslant n-1$, this proves that $X_i y^j|_{y^n=0} = 0$ for $m \leqslant j \leqslant n-1$. Thus condition (c) is also satisfied for the chart $(U, y^1, \ldots, y^n)$ (with $x^1, \ldots, x^n$ replaced by $y^1, \ldots, y^n$). $\square$

Proposition 7 now clearly follows from this lemma.

Let a chart $(U, x^1, \ldots, x^n)$ and fields $X_1, \ldots, X_m$ satisfy the hypotheses of Lemma 3.

Consider a Lie bracket $[X_m, X_i]$, $i = 1, \ldots, m-1$. By virtue of involutedness this vector field is in $\mathfrak{a}(E|_U)$ and hence there are smooth functions $c_i^1, \ldots, c_i^m$ on U such that

$$[X_m, X_i] = c_i^1 X_1 + \ldots + c_i^m X_m, \quad i = 1, \ldots, m-1,$$

and therefore

$$[X_m, X_i]\, x^j = c_i^1 X_1 x^j + \ldots + c_i^m X_m x^j$$

for any $j = 1., \ldots, n$. If $j \neq n$ (which is the only interesting case), then $X_m x^j = 0$. It may be assumed, therefore, that the last term at the right is of the form $c_i^{m-1} X_{m-1} x^j$. On the other hand, by definition of a Lie bracket

$$[X_m, X_i]\, x^j = X_m (X_i x^j) - X_i (X_m x^j) = \frac{\partial X_i x^j}{\partial x^m}$$

since under the hypothesis $X_m = \dfrac{\partial}{\partial x^m}$. This means that for any $j = 1, \ldots, n-1$ (and obviously for $j = n$) the functions

$$z_1 = X_1 x^j, \ldots, z_{m-1} = X_{m-1} x^j$$

as functions of $t = x^n$ are the solutions of a system of differential equations

$$\frac{dz_i}{dt} = c_i^1 z_1 + \ldots + c_i^{m-1} z_{m-1}, \quad i = 1, \ldots, m-1.$$

But according to condition (c) of Lemma 3, the functions $z_1, \ldots, z_{m-1}$ are zero for $t = 0$. Hence they are zero for any t.

This proves that on U the fields $X_1, \ldots, X_{m-1}$ are expressed in terms of the fields $\dfrac{\partial}{\partial x^1}, \ldots, \dfrac{\partial}{\partial x^{m-1}}$ and hence $X_1, \ldots, X_m$ are expressed in terms of the fields $\dfrac{\partial}{\partial x^1}, \ldots, \dfrac{\partial}{\partial x^{m-1}}, \dfrac{\partial}{\partial x^n}$. The last fields therefore form a basis of the module $\mathfrak{a}(E|_U)$.

To complete the induction step it remains to rewrite the coordinates x^n and x^m.

This completes the proof of Proposition 6 together with Proposition 5 and Lemma 2. □

Corollary. *A subfibering of a tangent bundle is integrable if and only if it is completely integrable.* □

Lecture 8

Coverings · Sections of coverings · Pointed coverings · Coamalgams · Simply connected spaces · Morphisms of coverings · The relation of quasi-order in the category of pointed coverings · The existence of simply connected coverings · Questions of substantiation · The functorial property of a universal covering

---

Now we proceed to study the localization functor GR_0-DIFF $\to$ GR-LOC. The investigation of this functor is based on an entirely different range of ideas and methods connected in the main with the so-called "covering spaces". The generally accepted presentation of the theory of covering spaces using the notion of "homotopic paths" has been explained many a time in textbooks and monographs, both regardless of applications to Lie group theory (see [13] chap. 5, for example) and in connection with that theory (see [8], chap. 9, for example). We shall present another, more elementary presentation of the theory, which was first proposed, in a somewhat different form, by Claude Chevalley, and uses nothing but the simplest general-topological constructions. We then apply the results obtained to the investigation of the localization functor.

Definition 1. Let $\pi: \tilde{X} \to X$ be a continuous surjective mapping of topological space $\tilde{X}$ onto topological space X and let $U \subset X$ be an open subset of X. We say that U is *evenly covered* by π if the inverse image $\pi^{-1}(U)$ of the set U under π is the union of disjoint open sets, each homeomorphically mapped by π onto U. The mapping π is said to be a *covering* of X if X and $\tilde{X}$ are connected and any

point of X has a neighbourhood evenly covered by π. The space $\tilde{X}$ is called a *covering space* in that case.

Sometimes we have to consider surjective mappings $\pi: \tilde{X} \to X$ for which X is connected and any point of X has a neighbourhood evenly covered by a mapping π but in general $\tilde{X}$ is not connected. Such mappings will be called *weak coverings.*

If U is evenly covered by a mapping π, then so is any open set $V \subset U$. Hence *for any (general weak) mapping* $\pi: \tilde{X} \to X$ *evenly covered open sets* $U \subset X$ *form a base of* X.

Since every point $\tilde{x} \in \tilde{X}$ is in the inverse image of some point $x \in X$, open sets $\tilde{U} \subset \tilde{X}$ which π homeomorphically maps onto open sets $U \subset X$ form a base of $\tilde{X}$, i.e. any open set of $\tilde{X}$ is a union of such sets.

A continuous mapping $\pi: \tilde{X} \to X$ that has the latter property is called a *local homeomorphism.* Thus *any (weak) covering is a local homeomorphism.*

Notice that the converse is not true. For example, the restriction of a covering $\pi: \tilde{X} \to X$ to a subspace $\tilde{X} \setminus \{\tilde{x}_0\}$, where $\tilde{x}_0 \in \tilde{X}$ is an arbitrary point (even if that restriction is surjective and the subspace $\tilde{X} \setminus \{\tilde{x}_0\}$ is connected) is a local homeomorphism which is not a covering.

Every local homeomorphism is obviously an open mapping (i.e. sends open sets into open sets). *Any (weak) covering* therefore *is an open mapping.*

In general the representation of the inverse image of an evenly covered set $U \subset X$ as a union of disjoint open sets $\tilde{U}_\alpha$, each homeomorphically mapped onto U, is by no means unique. But *it is so if U is connected*, for in that case the sets $\tilde{U}_\alpha$ may be characterized as the components of connectedness of the set $\pi^{-1}(U)$ (each of them, being homeomorphic to U, is connected, and they are open and disjoint sets).

Many of the important topological properties of a space X are inherited by any of its covering spaces $\tilde{X}$. For example,

it follows immediately from the fact that the covering $\pi: \widetilde{X} \to X$ is a local homeomorphism that $\widetilde{X}$ *is locally connected if* X *is.*

Similarly, *it is easy to see that if* X *is Hausdorff, then so is each covering space* $\widetilde{X}$ *of it.* Indeed, let $\widetilde{x}_1$, $\widetilde{x}_2$ be distinct points of $\widetilde{X}$. If $\pi(\widetilde{x}_1) = \pi(\widetilde{x}_2)$, then under the hypothesis $\widetilde{x}_1$ and $\widetilde{x}_2$ are in two disjoint open sets. But if $\pi(\widetilde{x}_1) \neq \pi(\widetilde{x}_2)$, then X being Hausdorff, $\pi(\widetilde{x}_1)$ and $\pi(\widetilde{x}_2)$ have disjoint neighbourhoods U_1 und U_2. The inverse images $\pi^{-1}(U_1)$ and $\pi^{-1}(U_2)$ of the neighbourhoods are precisely the disjoint open sets containing $\widetilde{x}_1$ and $\widetilde{x}_2$. $\square$

Let $U \subset X$ be an open set evenly covered by a mapping $\pi: \widetilde{X} \to X$. Consider disjoint open sets $\widetilde{U}_\alpha \subset \widetilde{X}$ on which π is homeomorphic and whose union is the set $\pi^{-1}(U)$. By definition, for any α the homeomorphism $\sigma_\alpha: U \to \widetilde{U}_\alpha$ inverse to the homeomorphism $\pi|_{\widetilde{U}_\alpha}: \widetilde{U}_\alpha \to U$ is a section of π over U (more precisely, the section is its composition with the embedding $\widetilde{U}_\alpha \to \widetilde{X}$).

On the other hand, we know that if U is connected, then U_α are uniquely defined and that to give any of them it is sufficient to indicate in the set some point (since these sets are the components of the set $\pi^{-1}(U)$). Sections σ_α are therefore also uniquely defined. This means that if we choose in U an arbitrary point x_0, then for any point $\widetilde{x}_\alpha \in \pi^{-1}(x_0)$ there will be a unique section $\sigma_\alpha: U \to \widetilde{X}$ of π over U for which $\sigma(\widetilde{x}_\alpha) = x_0$.

Conversely, let U be a connected subset of X with the property that for any point $x_0 \in U$ and any point $\widetilde{x}_\alpha \in \pi^{-1}(x_0)$ there is a unique section $\sigma_\alpha: U \to \widetilde{X}$ of π over U for which $\sigma_\alpha(x_0) = \widetilde{x}_\alpha$. Consider a point $\widetilde{x}$ of the set $\pi^{-1}(U)$. Let $x = \pi(\widetilde{x})$. Under the hypothesis there is a unique section $\sigma: U \to \widetilde{X}$ of π over U such that $\sigma(x) = \widetilde{x}$. Let $\sigma(x_0) = \widetilde{x}_\alpha$. Then, σ_α being unique, $\sigma = \sigma_\alpha$, which shows in

particular that $\tilde{x} \in \sigma_\alpha(U)$. Hence $\pi^{-1}(U)$ is the union of $\sigma_\alpha(U)$. If $\tilde{x} \in \sigma_{\alpha_1}(U) \cap \sigma_{\alpha_2}(U)$, then $\tilde{x}_{\alpha_1} = \sigma_{\alpha_1}(x_0) = \sigma(x_0) = \sigma_{\alpha_2}(x_0) = \tilde{x}_{\alpha_2}$ and therefore $\sigma_{\alpha_1} = \sigma_{\alpha_2}$. Hence distinct sets $\sigma_\alpha(U)$ do not intersect. Since $\sigma_\alpha(U)$ are connected (being homeomorphic to the connected set U), this proves that they are the components of the set $\pi^{-1}(U)$. If $\tilde{X}$ is locally connected, then those components must be open. Thus, under the assumptions made $\pi^{-1}(U)$ is decomposed as a union of disjoint open sets, each homeomorphically mapped onto U. In other words, the set U is evenly covered by the mapping π.

We have thus proved the following proposition:

Proposition 1. *If a space $\tilde{X}$ is locally connected, then a connected open set $U \subset X$ is evenly covered by a mapping π: $\tilde{X} \to X$ if and only if for any point $x_0 \in U$ and any point $\tilde{x}_\alpha \in \pi^{-1}(x_0)$ there is a unique section σ_α of π over U such that $\sigma_\alpha(x_0) = \tilde{x}_\alpha$.* $\square$

Corollary. *Let U and V be connected open sets of a space X, that are evenly covered by a mapping π: $\tilde{X} \to X$. If :*

(a) *$\tilde{X}$ is locally connected;*

(b) *the intersection $U \cap V$ is connected, then the set $U \cup V$ is also evenly covered by π.*

Proof. Let $x_0 \in U \cup V$ and $\tilde{x}_\alpha \in \pi^{-1}(x_0)$. If suffices to prove that there is a section σ_α: $U \cup V \to \tilde{X}$ of π over $U \cup V$ such that $\sigma_\alpha(x_0) = \tilde{x}_\alpha$ and that the section is unique. We may assume without loss of generality that $x_0 \in U$.

Under the hypothesis there is a section σ'_α: $U \to \tilde{X}$ of π over U, such that $\sigma'_\alpha(x_0) = \tilde{x}_\alpha$ and that section is unique. On choosing in $U \cap V$ a point y_0, consider the point $\tilde{y}_0 = \sigma'_\alpha(y_0) \in \tilde{X}$. Since $y_0 \in V$, there is a unique section σ''_α: $V \to \tilde{X}$ of π over V, such that $\sigma''_\alpha(y_0) = \tilde{y}_0$. Restrictions to $U \cap V$ of σ'_α and σ''_α are sections over $U \cap V$ that send y_0 to $\tilde{y}_0$. Since $U \cap V$ is connected, it follows that $\sigma'_\alpha = \sigma''_\alpha$ on $U \cap V$. Therefore σ'_α and σ''_α define on $U \cup V$ a con-

tinuous mapping σ_α: $U \cup V \to \widetilde{X}$ which is obviously a section such that $\sigma_\alpha(x_0) = \widetilde{x}_\alpha$.

The existence of the section σ_α is established. Its uniqueness is obvious now. $\square$

Proposition 1 (together with the corollary) applies in particular to any covering π: $\widetilde{X} \to X$ of a locally connected (and connected) space X.

Under the hypotheses of Proposition 1 the image $\sigma_\alpha(U)$ of the set U is under each of the mappings σ_α and open subset of the set $\widetilde{X}$. As shown by the following proposition, that fact is indeed of a very general character:

Proposition 2. *If X is a locally connected space, then for an arbitrary covering π: $\widetilde{X} \to X$ every section of it σ: $V \to \widetilde{X}$ over any open set $V \subset X$ is an open mapping.*

In particular, $\sigma(V)$ is an open set in $\widetilde{X}$ and σ is a homeomorphism of the set V onto $\sigma(V)$ (with the inverse homeomorphism $\pi|_{\sigma(V)}$).

Proof. Since over each open set in V the mapping σ is also a section, it suffices to prove that $\sigma(V)$ is open in $\widetilde{X}$.

Let $\widetilde{x} \in \sigma(V)$ and let $x \in V$ be a point such that $\sigma(x) = \widetilde{x}$. Also let U be a connected neighbourhood of x in V evenly covered by the mapping π and let $\widetilde{U}$ be a component of its inverse image $\pi^{-1}(U)$ containing the point $\widetilde{x}$. The image $\sigma(U)$ of U under σ is a connected set containing the point $\widetilde{x}$. Hence $\sigma(U) \subset \widetilde{U}$ and therefore a mapping $(\pi|_{\widetilde{U}}) \circ \sigma = \mathrm{id}$ is defined. But under the hypothesis the mapping $\pi|_{\widetilde{U}}$: $\widetilde{U} \to U$ is homeomorphic. Let σ': $U \to \widetilde{U}$ be the inverse homeomorphism. Then $\sigma' \circ (\pi|_{\widetilde{U}}) = \mathrm{id}$ and hence

$$\sigma' = \sigma' \circ (\pi|_{\widetilde{U}} \circ \sigma) = (\sigma' \circ \pi|_{\widetilde{U}}) \circ \sigma = \sigma.$$

In particular $\sigma(U) = \sigma'(U) = \widetilde{U}$. This means that the neighbourhood $\widetilde{U}$ of $\widetilde{x} \in \sigma(V)$ is entirely in $\sigma(V)$, so that $\widetilde{x}$ is an interior point of the set $\sigma(V)$. Hence $\sigma(V)$ is an open set. $\square$

The uniqueness of sections σ_α required in Proposition 1 can in fact be proved (in the only case of interest to us where π is a covering of a Hausdorff space). It is, however, convenient for us to prove uniqueness in a somewhat more general situation to describe which we introduce the following definition:

Definition 2. Let $f: Y \to X$ and $\pi: \tilde{X} \to X$ be two morphisms of an arbitrary category $\mathcal{C}$. The morphism $\tilde{f}: Y \to \tilde{X}$ of $\mathcal{C}$ is said to be a *lifting* of the morphism f (with respect to π) if $f = \pi \circ f$ i.e. if the diagram

$$\begin{tikzcd} & \tilde{X} \arrow[d, "\pi"] \\ Y \arrow[ur, "\tilde{f}"] \arrow[r, "f"'] & X \end{tikzcd}$$

is commutative.

Sections are nothing but liftings of the identity morphism $X \to X$ and sections over $U \subset X$ (in the case where $\mathcal{C}$ is the category TOP of topological spaces) are liftings of the embedding $U \to X$.

Proposition 3. *If $\pi: \tilde{X} \to X$ is a covering of a Hausdorff space X, then for an arbitrary continuous mapping $f: Y \to X$ of a connected space Y into a space X any two liftings of it $\tilde{f}, \tilde{f}': Y \to \tilde{X}$ that coincide at least at one point $y_0 \in Y$ will coincide everywhere.*

Proof. Let Y' be the set of all points $y \in Y$ such that $\tilde{f}y = \tilde{f}'y$. The set Y' is nonempty (contains a point y_0) and closed (for X is a Hausdorff space). Since under the hypothesis Y is a connected space, to prove Proposition 3 it therefore suffices to establish that Y' is also an open set.

Let $y \in Y'$ and let U be a neighbourhood of a point $f(y) \in X$ evenly covered by the mapping π. Then the point $\tilde{f}(y) = \tilde{f}'(y)$ has in $\tilde{X}$ a neighbourhood $\tilde{U}$ on which π is a homeomorphism $\tilde{U} \to U$. Since $\tilde{f}$ and $\tilde{f}'$ are continuous mappings, the point y has in Y a neighbourhood V such

that $\tilde{f}(V) \subset \tilde{U}$ and $\tilde{f}'(V) \subset \tilde{U}$. As π is homeomorphic on $\tilde{U}$ and as $\pi \circ \tilde{f} = \pi \circ \tilde{f}'$, we have $\tilde{f} = \tilde{f}'$ on V, i.e. $V \subset Y'$. Hence Y' is an open set. □

It is convenient to introduce at this point a general-topological definition.

Definition 3. A topological space X is said to be *pointed* if it has some base point x_0. The *mapping* $(X, x_0) \to (Y, y_0)$ of pointed space (X, x_0) into pointed space (Y, y_0) is a continuous mapping $X \to Y$ that sends point x_0 to point y_0.

Pointed spaces and their mappings form a category. This will be denoted by $\mathrm{TOP}^{\bullet}$.

A *pointed covering* is a mapping $\pi\colon (\tilde{X}, \tilde{x}_0) \to (X, x_0)$ of the category $\mathrm{TOP}^{\bullet}$ which is a covering as a mapping $\tilde{X} \to X$ of the category TOP.

In this terminology Proposition 3 states that *a mapping $f\colon (Y, y_0) \to (X, x_0)$ of connected pointed space (Y, y_0) into Hausdorff pointed space (X, x_0) admits with respect to the pointed covering $\pi\colon (\tilde{X}, \tilde{x}_0) \to (X, x_0)$ at most one lifting $\tilde{f}\colon (Y, y_0) \to (\tilde{X}, \tilde{x}_0)$.*

In what follows, for simplicity of notation we shall simply write X, $\tilde{X}$ etc. instead of (X, x_0), $(\tilde{X}, \tilde{x}_0)$, etc., explicitly indicating base points only when it is impossible to do without.

Suppose again that $f\colon Y \to X$ and $\pi\colon \tilde{X} \to X$ are morphisms of a category $\mathbf{C}$ and that those morphisms are included in a commutative diagram of the form

$$\begin{tikzcd} Y_f \arrow[r, "f^*"] \arrow[d, "\pi_f"'] & \tilde{X} \arrow[d, "\pi"] \\ Y \arrow[r, "f"'] & X \end{tikzcd}$$

That diagram is said to be a *universal square* and the morphism $\pi_f\colon Y_f \to Y$ (or the object Y_f) is a *coamalgam* of the morphisms f and π (or the objects Y and $\tilde{X}$ over the object X),

if for any object Z and any morphisms g_1: $Z \to Y$ and g_2: $Z \to \widetilde{X}$ that satisfy the relation

(1) $$f \circ g_1 = \pi \circ g_2$$

there is a unique morphism g: $Z \to Y_f$ such that

(2) $$\pi_f \circ g = g_1, \quad f^* \circ g = g_2,$$

i.e., in other words, if any commutative diagram of the form

$$\begin{tikzcd}
Y_f \arrow[rr, dashed] \arrow[dd] & & \widetilde{X} \arrow[dd, dashed] \\
& Z \arrow[ur] \arrow[dl] \arrow[dr] & \\
Y \arrow[rr] & & X
\end{tikzcd}$$

is uniquely supplemented to a commutative diagram of the form

$$\begin{tikzcd}
Y_f \arrow[rr] \arrow[dd] & & \widetilde{X} \arrow[dd] \\
& Z \arrow[ul] \arrow[ur] \arrow[dl] \arrow[dr] & \\
Y \arrow[rr] & & X
\end{tikzcd}$$

Any two coamalgams Y_f and Y_f' of given morphisms f and π are naturally isomorphic: there is one and only one isomorphism $Y_f \to Y_f'$ that closes the commutative diagram

$$\begin{tikzcd}
Y_f \arrow[rr] \arrow[dr, "\pi_f"'] & & Y_f' \arrow[dl, "\pi_f'"] \\
& Y &
\end{tikzcd}$$

The basic property of the coamalgam π_f: $Y_f \to Y$ is that *its sections* g: $Y \to Y_f$ *are in natural bijective correspondence with liftings* $\widetilde{f}: Y \to \widetilde{X}$ *of the morphism* f. Indeed,

every section g gives a lifting $f^* \circ g$, and for every lifting $\tilde{f}$ morphisms $g_1 = \mathrm{id}$ and $g_2 = \tilde{f}$ satisfy (with $Z = Y$) conditions (1) and hence define a morphism $g\colon Y \to Y_f$ which is (by virtue of the first relation of (2)) a section of the morphism π_f. $\square$

In that sense liftings reduce to their special case, sections.

This presupposes, of course, the existence of the coamalgam π_f. It turns out that in the case we are interested in, that of the category TOP· (or TOP·), the *coamalgam* π_f: $Y_f \to Y$ *exists for any continuous mappings* $f\colon Y \to X$ *and* $\pi\colon \tilde{X} \to X$. A subspace of the direct product $Y \times \tilde{X}$ consisting of points $(y, \tilde{x})$ such that $f(y) = \pi(\tilde{x})$ is the corresponding space Y_f and the mappings π_f and f^* are restrictions of projections of that product onto its factors. The fact that this does indeed give a coamalgam can immediately be verified: if $f \circ g_1 = \pi \circ g_2$, then the mapping $g = g_1 \times g_2\colon Z \to Y \times \tilde{X}$ is a mapping into Y_f and satisfies $\pi_f \circ g = g_1$ and $f^* \circ g = g_2$; on the other hand, since π_f and f^* are the projections, these relations uniquely characterize the mapping g. $\square$

Lemma 1. *If a mapping* $\pi\colon \tilde{X} \to X$ *is a (weak) covering, then for any mapping* $f\colon Y \to X$ *the coamalgam*

$$\pi_f\colon Y_f \to Y$$

is a weak covering.

Proof. The mapping π_f is surjective, since for any point $y \in Y$ there is a point $\tilde{x} \to \tilde{X}$ such that $\pi(\tilde{x}) = f(y)$. Let U be an open subset of a space X that is evenly covered by the mapping π and let $V = f^{-1}(U)$ be the inverse image of the set U under the mapping f. It is clear that

$$\pi_f^{-1}(V) = Y_f \cap (V \times \pi^{-1}(U)).$$

If therefore

$$\pi^{-1}(U) = \bigcup_{\alpha} \tilde{U}_\alpha,$$

where $\tilde{U}_\alpha$ are disjoint open subsets of a space $\tilde{X}$ that are homeomorphically mapped onto U, then

$$\pi_f^{-1}(V) = \bigcup_\alpha V_\alpha,$$

where

$$V_\alpha = Y_f \cap (V \times \tilde{U}_\alpha).$$

The sets V_α are open, do not intersect and are homeomorphically mapped by means of π_f onto V. Hence, the set V is evenly covered by π_f. To complete the proof it remains to notice that sets of the form V cover the entire Y. □

Thus, if we are to obtain a covering it suffices to go from the space Y_f to some component of it. That we do indeed obtain a covering is shown by the following lemma:

Lemma 2. *If X is a connected and locally connected space, then for any weak covering π: $\tilde{X} \to X$ and any component $\tilde{X}_0$ of a space $\tilde{X}$ the mapping*

$$\pi_0 = \pi|_{\tilde{X}_0}: \tilde{X}_0 \to X$$

is a covering.

Proof. Let U be a connected open subset of a space X, that is evenly covered by a mapping π. Those of the components of the set $\pi^{-1}(U)$ that intersect $\tilde{X}_0$ are necessarily in $\tilde{X}_0$ (by virtue of connectedness). If, therefore, $\pi_f(\tilde{X}_0) \cap U \neq \varnothing$, then $U \subset \pi(\tilde{X}_0)$. Since sets of the form U form a base of X, this shows that the nonempty set $\pi(\tilde{X}_0)$ is at the same time open and closed. Hence it exhausts all X, so that π_0 is a surjective mapping. Since $\pi_0^{-1}(U)$ is the union of the components of $\pi^{-1}(U)$ that are in $\tilde{X}_0$, the mapping π_0 evenly covers the set U. Hence π_0 is a covering. □

Now consider the question of the existence of liftings (and sections). Here we must begin from afar.

Any homeomorphism π: $\tilde{X} \to X$ is clearly a covering.

Definition 4. A covering π: $\tilde{X} \to X$ which is a homeomorphism of a space $\tilde{X}$ onto X is called *trivial*.

Proposition 4. *A covering* $\pi\colon \widetilde{X} \to X$ *of a locally connected (and connected) space* X *is trivial if and only if it has a section* $\sigma\colon X \to \widetilde{X}$ *over the whole of* X.

Proof. If π is trivial, then σ is the inverse homeomorphism $X \to \widetilde{X}$ (regardless of whether or not X is locally connected).

Conversely, let the covering $\pi\colon \widetilde{X} \to X$ have a section $\sigma\colon X \to \widetilde{X}$. By Proposition 2 that section is a homeomorphism of a space X onto an open subset $\sigma(X)$ of $\widetilde{X}$ with an inverse homeomorphism $\pi|_{\sigma(X)}\colon \sigma(X) \to X$. To prove Proposition 4 therefore it suffices to establish that $\sigma(X) = \widetilde{X}$. Since $\widetilde{X}$ is connected and $\sigma(X)$ is an open and nonempty set, this will be proved if we show that $\sigma(X)$ is closed in $\widetilde{X}$.

Let $\widetilde{x}$ be a point of closure $\overline{\sigma(X)}$ of $\sigma(X)$ and let U be a neighbourhood of a point $x = \pi(\widetilde{x})$ that is evenly covered by a mapping π. Consider an open set $\widetilde{U}$ containing the point $\widetilde{x}$ and mapped homeomorphically onto U. Since $\widetilde{x} \in \overline{\sigma(X)}$, the intersection $\widetilde{U} \cap \sigma(X)$ is not empty. Let $\widetilde{y} \in \widetilde{U} \cap \sigma(X)$. Since the mapping $\pi|_{\sigma(X)}\colon \sigma(X) \to X$ is a homeomorphism, there is an open set $\widetilde{U}'$ in $\sigma(X)$ which is mapped homeomorphically onto U and contains a point $\widetilde{y}$. Since U is evenly covered, $\widetilde{U}$ and $\widetilde{U}'$ either coincide or do not intersect. But they have a point $\widetilde{y}$ in common. Hence $\widetilde{U}' = \widetilde{U}$ and therefore $\widetilde{x} \in \widetilde{U} = \widetilde{U}' \subset \sigma(X)$. Thus the set $\sigma(X)$ is closed. $\square$

Definition 5. A connected space X is said to be *simply connected* if any covering of it is trivial.

The significance of simply connected spaces for the problem of the existence of liftings is determined by the following theorem:

Theorem 1. *Let* $\pi\colon (\widetilde{X}, \widetilde{x}_0) \to (X, x_0)$ *be a pointed covering of a pointed Hausdorff space* (X, x_0) *and let* (Y, y_0) *be a connected, locally connected and simply connected pointed space.*

Then for any mapping $f\colon (Y, y_0) \to (X, x_0)$ there is a unique lifting $\tilde{f}\colon (Y, y_0) \to (\tilde{X}, \tilde{x}_0)$.

Proof. By definition $(y_0, \tilde{x}_0) \in Y_f$. Let $(Y_f)_0$ be a component of Y_f containing a point $(y_0, \tilde{x}_0)$. By Lemma 2 the mapping $(\pi f)_0 = \pi_f|_{(Y_f)_0}\colon (Y_f)_0 \to Y$ is a covering. Hence, Y being simply connected, that mapping is a homeomorphism. If $(\pi_f)_0^{-1}\colon Y \to (Y_f)_0$ is the inverse homeomorphism, then the mapping

$$\tilde{f} = f^* \circ (\pi_f)_0^{-1}\colon Y \to \tilde{X}$$

is a lifting of the mapping f that satisfies the relation $\tilde{f}(y_0) = \tilde{x}_0$. The uniqueness of the lifting $\tilde{f}$ is ensured by Proposition 3. □

Corollary 1. *An arbitrary covering $\pi\colon \tilde{X} \to X$ of a connected, locally connected and Hausdorff space X evenly covers every open simply connected subset $U \subset X$.*

Proof. It is sufficient to use Proposition 1. □

Corollary 2. *A connected and locally connected Hausdorff space X is simply connected if it is the union of doubly connected and simply connected open sets U and V whose intersection $U \cap V$ is connected.*

Proof. By Corollary 1 every covering $\pi\colon \tilde{X} \to X$ evenly covers both U and V. Therefore (Corollary 1 to Proposition 1) it evenly covers $X = U \cup V$ and is therefore trivial. □

Definition 6. A *morphism* of a covering $\pi_1\colon \tilde{X}_1 \to X$ into a covering $\pi_2\colon \tilde{X}_2 \to X$ is a continuous mapping $f\colon \tilde{X}_1 \to \tilde{X}_2$ such that there is a commutative diagram

$$\begin{tikzcd} \tilde{X}_1 \arrow[rr, "f"] \arrow[dr, "\pi_1"'] & & \tilde{X}_2 \arrow[dl, "\pi_2"] \\ & X & \end{tikzcd}$$

It is clear that all coverings (of a given connected space X) and all their morphisms form a category. This will be denoted by COV (X).

Similarly defined is the category of *pointed coverings* COV (X, x_0) whose morphisms are morphisms of COV (X) that are at the same time mappings of pointed spaces. The category COV (X, x_0) will be denoted also by $\mathrm{COV}^{\bullet}(X)$.

Clearly, the morphism $f\colon \tilde{X}_1 \to \tilde{X}_2$ *of* COV (X) *(or* COV (X, x_0)*) is an isomorphism (has an inverse morphism) if and only if it is a homeomorphism of a space* $\tilde{X}_1$ *onto* $\tilde{X}_2$.

A covering $\pi\colon \tilde{X} \to X$ is trivial (in the sense of Definition 4) if and only if it is isomorphic in COV (X) to the identity covering id: $X \to X$.

Lemma 3. *If a connected space* X *is locally connected, then any morphism* $f\colon \tilde{X}_1 \to \tilde{X}_2$ of COV (X) (or COV (X, x_0)) *is itself a covering* (*of* $\tilde{X}_2$).

Proof. Let $\{U_\alpha\}$ be a base of the space X that is made up of connected open sets evenly covered by mappings $\pi_1\colon \tilde{X}_1 \to X$ and $\pi_2\colon \tilde{X}_2 \to X$ at the same time, and let $\tilde{U}^{(1)}_{\alpha,\beta}$ be components of the inverse image $\pi_1^{-1}(U_\alpha)$ of a set U_α under π_1 and let $\tilde{U}^{(2)}_{\alpha,\gamma}$ be components of the inverse image $\pi_2^{-1}(\tilde{U}_\alpha)$ of U_α under π_2. Since $\pi_1 = \pi_2 \circ f$, each of the sets $\tilde{U}^{(1)}_{\alpha,\beta}$ is homeomorphically mapped by means of f onto some set $\tilde{U}^{(2)}_{\alpha,\gamma}$. If therefore for some α and γ the set $\tilde{U}^{(2)}_{\alpha,\gamma}$ intersects a subspace $f(\tilde{X}_1)$, then it is necessarily contained therein: $\tilde{U}^{(2)}_{\alpha,\gamma} \subset f(\tilde{X}_1)$. Since sets of the form $\tilde{U}^{(2)}_{\alpha,\gamma}$ form a base of the space X_2, this is possible only when the subspace $f(\tilde{X}_1)$ is both closed and open. Hence $f(\tilde{X}_1) = \tilde{X}_2$, so that the mapping f is surjective.

In addition, we see that for any set $\tilde{U}^{(2)}_{\alpha,\gamma}$ its inverse image $f^{-1}(\tilde{U}^{(2)}_{\alpha,\gamma})$ under f is the union of some (in fact all) sets of the form $\tilde{U}^{(1)}_{\alpha,\beta}$ the mapping f being a homeomorphism on each of these sets. Thus each of the sets $\tilde{U}^{(2)}_{\alpha,\gamma}$ is evenly covered by the mapping f. Hence f is a covering. □

Every morphism f of a covering $\pi_1\colon \tilde{X}_1 \to X$ into $\pi_2\colon \tilde{X}_2 \to X$ is nothing but a lifting of the mapping $\pi_1\colon \tilde{X}_1 \to X$ with respect to π_2. In view of Proposition 3 therefore, *if* X

is a Hausdorff space, then for any two pointed coverings π_1: $(\tilde{X}, \tilde{x}_1) \to (X, x_0)$ *and* π_2: $(\tilde{X}_2, \tilde{x}_2) \to (X, x_0)$ *there is at most one morphism of covering* π_1 *into covering* π_2 *in* COV (X, x_0).

In particular, for every covering π: $(\tilde{X}, \tilde{x}_0) \to (X, x_0)$ there is only one morphism $\pi \to \pi$, the identity morphism.

We shall write $\pi_1 \geqslant \pi_2$ if the morphism $\pi_1 \to \pi_2$ exists. It is clear that this relation on the set of all pointed coverings of the set (X, x_0) is reflexive and transitive, i.e. is the *relation of quasi-order.*

We say that pointed coverings π_1 and π_2 are *equivalent* if at the same time $\pi_1 \geqslant \pi_2$ and $\pi_2 \geqslant \pi_1$. It is clear that on all classes of equivalent coverings the relation $\geqslant$ induces the *relation of order*. It is easy to see that *if X is a Hausdorff space, then π_1 and π_2 are equivalent if and only if they are isomorphic.* Indeed, isomorphic coverings are obviously equivalent. Conversely, if π_1 and π_2 are equivalent coverings, i.e. if there are morphisms f: $\pi_1 \to \pi_2$ and g: $\pi_2 \to \pi_1$, then by virtue of uniqueness the morphisms $f \circ g$: $\pi_2 \to \pi_2$ and $g \circ f$: $\pi_1 \to \pi_1$ are identity morphism id: $\pi_2 \to \pi_2$ and id: $\pi_1 \to \pi_1$ and hence f and g are mutually inverse isomorphisms. □

Thus *if X is a Hausdorff space, then the relation of order* $\geqslant$ *is defined on classes of isomorphic objects of the category* COV (X, x_0) (with any selected point x_0).

Definition 7. A pointed covering π_0: $(\tilde{X}_0, \tilde{x}_0) \to (X, x_0)$ of a pointed Hausdorff space (X, x_0) is said to be:

(a) *universal* if $\pi_0 \geqslant \pi$ for any pointed covering π: $(\tilde{X}, \tilde{x}) \to (X, x_0)$;

(b) *maximal* if $\pi \geqslant \pi_0$ if and only if $\pi_0 \geqslant \pi$, i.e. if and only if π and π_0 are isomorphic;

(c) *simply connected* if $\tilde{X}_0$ is a simply connected space.

It is obvious that:

(a) *any two universal coverings are equivalent and hence isomorphic*;

(b) *every universal covering is maximal*;

(c) *if X is a locally connected space, then any simply connected covering is universal.*

Notice that the converses of these statements are in general false: there are locally connected spaces X with maximal but not universal and with universal but not simply connect-

ed coverings. There are also spaces with nonisomorphic maximal coverings.

It is clear, however, that if there is a universal covering π_0 of a space X, then any maximal covering of X is isomorphic to π_0, so that in this case maximal coverings coincide with universal ones.

In particular, if for a locally connected space X there is a simply connected covering π_0, then any maximal covering of it is isomorphic to π_0, so that for such spaces simply connected, universal and maximal coverings are the same.

Definition 8. A connected space X is said to be *semilocally simply connected* if there is an open covering for it made up of simply connected sets.

Theorem 2. *For any Hausdorff connected locally connected and semilocally simply connected space X there is a simply connected covering.*

Corollary 1. *For every Hausdorff connected locally connected and semilocally simply connected space the simply connected, or universal or maximal coverings are the same.* □

To prove Theorem 2 we shall need one general construction which is a generalized construction of a coamalgam of a pair of mappings.

Let A be some index set and let some (as yet arbitrary) continuous mapping $\pi_\alpha\colon \tilde{X}_\alpha \to X$ be given for any $\alpha \in$ A. Consider in the product $\prod\limits_\alpha X_\alpha$ of spaces $\tilde{X}_\alpha$ a subspace $\tilde{X}$ consisting of all points $(\tilde{x}_\alpha)$, $\tilde{x}_\alpha \in \tilde{X}_\alpha$ such that a point $\pi_\alpha(\tilde{x}_\alpha) \in X$ is the same for all α. Then the formula

$$\pi(\{\tilde{x}_\alpha\}) = \pi_\alpha(\tilde{x}_\alpha)$$

defines a continuous mapping

$$\pi\colon \tilde{X} \to X$$

called a *coamalgam* of mappings π_α. If all the spaces under consideration have base points and the mappings π_α are mappings of such spaces, then by taking a point $(\tilde{x}_\alpha^{(0)})$, where $\tilde{x}_\alpha^{(0)}$ are base points of spaces $\tilde{X}_\alpha$, as a base point of

the space $\widetilde{X}$ we see that the mapping π is also a mapping of the spaces with base points.

Suppose now that X is a connected, locally connected and Hausdorff space and that all mappings π_α are (pointed) coverings. Then by Corollary 1 to Theorem 1 any simply connected subset U of X is evenly covered by each of the mappings π_α. Let $\widetilde{U}_{\alpha, \beta_\alpha}$ be components of the set $\pi^{-1}(U_\alpha)$, where β_α ranges over some (α-dependent) index set B_α. Under the hypothesis every mapping

$$\pi_\alpha|_{\widetilde{U}_{\alpha, \beta_\alpha}} : \widetilde{U}_{\alpha, \beta_\alpha} \to U$$

is a homeomorphism and $\widetilde{U}_{\alpha, \beta_\alpha}$ are open and disjoint sets.

Let $B = \coprod_\alpha B_\alpha$ be the product of all sets B_α. For any $\beta = (\beta_\alpha) \in B$ we set

$$\widetilde{U}_\beta = \widetilde{X} \cap \coprod_\alpha \widetilde{U}_{\alpha, \beta_\alpha}.$$

It is clear that the sets $\widetilde{U}_\beta \subset \widetilde{X}$ are disjoint and together constitute the entire inverse image $\pi^{-1}(U)$ of the set U under the mapping π:

$$\pi^{-1}(U) = \bigcup_{\beta \in B} \widetilde{U}_\beta.$$

It is just as clear that on any set $\widetilde{U}_\beta$ the mapping π is a homeomorphism onto U (the inverse homeomorphism is the mapping $x \mapsto (\sigma_{\alpha, \beta_\alpha}(x))$, where $\sigma_{\alpha, \beta_\alpha}: U \to U_{\alpha, \beta_\alpha}$ is the homeomorphism inverse to $\pi_\alpha|_{U_{\alpha, \beta_\alpha}}$). In particular we see that the sets $\widetilde{U}_\beta$ are connected and are therefore the components of the set $\pi^{-1}(U)$.

We cannot, however, say that π evenly covers the set U, since $\widetilde{U}_\beta$ are in general not open subsets of the space $\widetilde{X}$.

To rectify the matter, we introduce into $\widetilde{X}$ a new, stronger topology (the one having a greater number of open sets). To give a topology on a set it suffices, of course, to give its base and it is known (and trivial to prove) that a family is

a base of some topology if and only if for any two sets V_1 and V_2 of that family the intersection $V_1 \cap V_2$ is the union of sets of the family. This characteristic property of bases is obviously satisfied for a family of sets that are the components of open sets of a topological space $\tilde{X}$ (if V_1 and V_2 are the components of open sets U_1 and U_2, then $V_1 \cap V_2$ consists of the components of the open set $U_1 \cap U_2$). Hence we can take that family as a base of some topology on $\tilde{X}$. A space $\tilde{X}$ provided with that topology will be denoted by $\tilde{X}'$ and by π' a mapping π considered as the mapping $\tilde{X}' \to X$. Since the sets open in $\tilde{X}$ are obviously so in $\tilde{X}'$, the mapping π' is continuous.

Since the sets $\tilde{U}_\beta$ are the components of the open set $\pi^{-1}(U)$, they are open in $\tilde{X}'$. But we cannot yet say that π' evenly covers the set X, since we cannot rule out the possibility that in going from $\tilde{X}$ to $\tilde{X}'$ the mapping π may lose the property of being a homeomorphism on $\tilde{U}_\beta$. In fact this does not happen, i.e. the mapping π' remains a homeomorphism on $\tilde{U}_\beta$. To put it another way, the topology on $\tilde{U}_\beta$ induced by the topology of the space X' (denote this topology by II) coincides with the original topology induced by the topology of $\tilde{X}$ (to be denoted by I). Indeed, in topology I the set $\tilde{U}_\beta$, being homeomorphic to the open set U of a locally connected set X, is itself locally connected, i.e. has a base compound of connected sets. On the other hand, in topology II any open set in $\tilde{U}_\beta$ is of the form $C \cap \tilde{U}_\beta$, where C is a component of some open set V in $\tilde{X}$. Let $\tilde{x}$ be an arbitrary point in $C \cap \tilde{U}_\beta$. The intersection $V \cap \tilde{U}_\beta$ is a neighbourhood of that point in I and hence contains some connected (and therefore contained in C) neighbourhood W of the point $\tilde{x}$. Thus every point $\tilde{x}$ in $C \cap \tilde{U}_\beta$ has in I a neighbourhood W contained in $C \cap \tilde{U}_\beta$. This means that the set $C \cap \tilde{U}_\beta$ is open in topology I. Hence topologies I and II coincide.

This proves that $\pi'\colon \widetilde{X}' \to X$ evenly covers every simply connected open subset $U \subset X$. If, therefore, X is a semilocally simply connected space, then any point of it has a neighbourhood evenly covered by π'. Hence π' is a weak covering and therefore for any component $\widetilde{X}_0'$ of X_0' the mapping

$$\pi_0' = \pi\,|_{\widetilde{X}_0'}\colon \widetilde{X}_0' \to X$$

is a covering. When we consider pointed coverings the component $\widetilde{X}_0'$ cannot be chosen arbitrarily since we should take as $\widetilde{X}_0'$ the component containing the base point $\widetilde{x}_0' = (x_\alpha^{(0)}) \in \widetilde{X}$.

Thus if X is a connected, locally connected and semilocally simply connected space, then the construction presented allows one to uniquely construct from any family of pointed coverings $\pi_\alpha\colon (\widetilde{X}_\alpha, \widetilde{x}_\alpha^{(0)}) \to (X, x_0)$ some pointed covering

$$\pi_0'\colon (\widetilde{X}_0', \widetilde{x}_0') \to (X, x_0).$$

Admitting inexact terminology, we shall call that covering a *coamalgam of coverings* π_α.

It is clear that the mapping $f_\alpha\colon \widetilde{X}_0' \to \widetilde{X}_\alpha$ defined by the formula

$$f_\alpha\,((\widetilde{x}_\alpha)) = \widetilde{x}_\alpha$$

is continuous and satisfies $\pi_0' = \pi_\alpha' \circ f_\alpha$, i.e. is a morphism of π_0' into a covering π_α. Thus, *if* π_0' *is a coamalgam of coverings* π_α, *then* $\pi_0' \geqslant \pi_\alpha$, *for any* $\alpha \in A$.

If therefore $\pi_\alpha\colon \widetilde{X}_\alpha \to X$ constitute a *complete family of pointed coverings*, i.e. if any pointed covering $\pi\colon \widetilde{X} \to X$ of X is isomorphic to some covering π_{α_0} (the existence of such a family is obvious: it suffices to choose in every class of isomorphic coverings of X one representative), then the covering $\pi_0'\colon X_0' \to X$ is universal. This proves that *for any connected locally connected and semilocally simply connected space* X *there is a universal covering* $\pi_0'\colon \widetilde{X}_0' \to X$.

Theorem 2 will now be proved if we show that for a Hausdorff space X that covering is simply connected. To do this we shall need the following lemma:

Lemma 4. *If a connected, locally connected and semilocally simply connected space X is Hausdorff, then the composition*

$$\pi \circ \rho: \ \widetilde{X}_1 \to X$$

of any two coverings π: $\widetilde{X} \to X$ and ρ: $\widetilde{X}_1 \to \widetilde{X}$ is also a covering.

Proof. Under the hypothesis, X has a covering composed of simply connected open sets U. By Corollary 1 to Theorem 1 the sets U are evenly covered by a mapping π and therefore the components $\widetilde{U}$ of their inverse images $\pi^{-1}(U)$ are open sets homeomorphic to sets U. Hence the space $\widetilde{X}$ is semilocally simply connected. In addition, under the hypothesis it is connected and according to the remarks made at the beginning of this lecture it is locally connected and Hausdorff. Therefore Corollary 1 to Theorem 1 applies again to the sets $\widetilde{U}$ and hence each of them is evenly covered by the mapping ρ. But then it is clear that the mapping $\pi \circ \rho$ will evenly cover all the sets U and will therefore be a covering of the space X. □

Now we are in a position to complete the proof of Theorem 2.

Lemma 5. *For any Hausdorff connected locally connected and semilocally simply connected space X the universal covering*

$$\pi_0': \widetilde{X}_0' \to X$$

which is a coamalgam of a complete family of coverings π_α: $\widetilde{X}_\alpha \to X$, is simply connected.

Proof. Let ρ: $\widetilde{X}_1 \to \widetilde{X}_0'$ be a pointed covering of the space $\widetilde{X}_0'$. By Lemma 4 the composition $\pi_0' \circ \rho$: $\widetilde{X}_1 \to X$ is a covering and is therefore (the family $\{\pi_\alpha\}$ being complete) isomorphic to some covering π_α: $\widetilde{X}_{\alpha_0} \to X$. Let f: $\widetilde{X}_{\alpha_0} \to \widetilde{X}_1$ be the corresponding isomorphism. Then the mapping $\rho \circ f$: $\widetilde{X}'_{\alpha_0} \to \widetilde{X}_0'$ is a morphism of π_{α_0} into π_0', so that $\pi_{\alpha_0} \geqslant \pi_0'$.

Since by virtue of universality $\pi'_0 \geqslant \pi_{\alpha_0}$ this proves that the coverings π_{α_0} and π'_0 are equivalent and hence isomorphic. If now $g: \tilde{X}_0 \to \tilde{X}_{\alpha_0}$ is an isomorphism of π'_0 onto π_{α_0} then the mapping $\sigma = f \circ g: \tilde{X}'_0 \to \tilde{X}_1$ is obviously a section of the covering ρ.

Hence by Proposition 6 ρ is a trivial covering.

Thus any covering of the space $\tilde{X}'_0$ is trivial, i.e. this space is simply connected. □

The above proof of Theorem 2 may give rise to doubts in connection with the notion of a complete family of coverings in whose definition there appear "all" coverings, which is known to lead to paradoxes (by the way this applies to the notion of a simply connected space as well in the definition of which there also appear "all" coverings of that space, but not to interrupt the presentation we have chosen not to dwell on that point there).

It is customary to assume within the framework of the scope of usual "naive" theory of sets that no paradoxes arise if we deal only with subsets of some fixed set and with their factor sets. With this in mind (and assuming a given pointed space (X, x_0) to be fixed) we consider the set Σ of all finite sequences of the form

$$(x_1, U_1, \ldots, x_n, U_n), \tag{3}$$

where $x_1, \ldots, x_n$ are points of a space X and $U_1, \ldots, U_n$ are its open subsets such that for any $i = 1, \ldots, n$ the points x_{i-1} and x_i are in U_i. In that set we consider subsets Σ' that have the following properties:

(i) there is a simply connected neighbourhood U of the point x_0 in X, such that $(x_0, U) \in \Sigma'$;

(ii) there is a factor set $\tilde{X} = \Sigma'/\varphi$ of a set Σ', a topology on that factor set and a continuous mapping $\pi: \tilde{X} \to X$ such that:

(a) π is a covering;

(b) all points of Σ' which have the form (x_0, U), where U is a simply connected neighbourhood of x_0 in X, define the same point $\tilde{x}_0$ of the factor set $\tilde{X}$ and π sends that point to x_0 (so that $\pi: (\tilde{X}, \tilde{x}_0) \to (X, x_0)$).

Let π_α: $(\widetilde{X}_\alpha, \widetilde{x}_\alpha) \to (X, x_0)$ be all pointed coverings of the form $\Sigma'/\varphi \to X$ that result from all possible choices of the subset Σ', the equivalence relation φ on Σ', the topology on Σ'/φ and the mapping π.

Lemma 6. *A family of pointed coverings π_α: $X_\alpha \to X$ is complete.*

Proof. Let π: $\widetilde{X} \to X$ be a pointed covering of a space X and let Σ' be the subset of Σ, which is composed of all sequences (3) for which all sets $U_1, \ldots, U_n$ are evenly covered by the mapping π. Consider an arbitrary sequence (3) in Σ'. We associate the point x_0 with a distinguished point $\widetilde{x}_0$ of the space $\widetilde{X}$. Under the hypothesis $\pi(\widetilde{x}_0) = x_0$. Proceeding by induction assume that for some $i = 1, \ldots, n$ we have already constructed a point $\widetilde{x}_{i-1} \in X$ having the property that $\pi(\widetilde{x}_{i-1}) = x_{i-1}$. Since the set U_i is evenly covered by the mapping π and since $x_{i-1} \in U_i$, there is a unique open set $\widetilde{U}_i$ in $\widetilde{X}$ containing $\widetilde{x}_{i-1}$ and homeomorphically mapped onto the set U_{i-1}. Since $x_i \in U_i$, there exists a unique point $\widetilde{x}_i$ in $\widetilde{U}_i$ for which $\pi(\widetilde{x}_i) = x_i$. Thus points $\widetilde{x}_i$ are constructed by induction for all $i = 1, \ldots, n$. In particular, a point $\widetilde{x}_n$ is constructed.

Notice that $\widetilde{x}_n$ is uniquely defined by sequence (3). Therefore the formula

$$\varphi(x_1, U_1, \ldots, x_n, \quad U_n) = \widetilde{x}_n$$

correctly defines some mapping of the set Σ' into the set $\widetilde{X}$. If that mapping is surjective, then the factor set Σ'/φ of Σ' it defines is in bijective correspondence with $\widetilde{X}$. We carry, with the aid of this correspondence, the topology of $\widetilde{X}$ and the mapping π over to Σ'/φ. All the conditions imposed above will clearly hold, so that we obtain some covering of the family $\{\pi_\alpha\}$. Since by construction that covering is isomorphic to a given covering π, we thus see that to complete the proof of Lemma 6 it remains for us to establish that the mapping φ: $\Sigma' \to \widetilde{X}$ is surjective.

To this end, consider the image $\varphi(\Sigma')$ of the set Σ' under mapping φ. If sequence (3) is in Σ', then on replacing in it the point x_n by a point of the set U_n we again obtain a sequence in Σ'. This shows that together with the point $\tilde{x}_n$ the set $\varphi(\Sigma')$ contains the whole of its neighbourhood $\tilde{U}_n$ (see above). Hence $\varphi(\Sigma')$ is open.

Now let $\tilde{x}$ be an arbitrary point of closure $\overline{\varphi(\Sigma')}$ of the set $\varphi(\Sigma')$ and let U be a neighbourhood of $x = \pi(\tilde{x})$ evenly covered by a mapping π and $\tilde{U}$ be a neighbourhood of $\tilde{x}$, which is homeomorphically mapped onto U. Since $\tilde{x} \in \overline{\varphi(\Sigma')}$, we have $\varphi(\Sigma') \cap \tilde{U} \neq \varnothing$. This means that there exists a sequence (3) in Σ', such that $\tilde{x}_n \in \tilde{U}$ and hence $x_n \in U$. Therefore the sequence

$$(x_1, U_1, \ldots, x_n, U_n, x, U)$$

is in Σ' and its image under φ is $\tilde{x}$. Thus $\tilde{x} \in \varphi(\Sigma')$ and hence the set $\varphi(\Sigma')$ is closed.

The set $\varphi(\Sigma')$ being an open and closed (nonempty) subset of a connected space $\tilde{X}$ coincides with the entire $\tilde{X}$, so that φ is surjective.

This completes the proof of Lemma 6. □

At the same time, according to the general principle given above this completely (within the "naive" theory of sets) justifies the construction of a universal simply connected covering. That a complete constructed family explicitly contains iterations (isomorphic coverings) is not relevant since we did not depend on the absence of iterations in a complete family when proving Theorem 2. However, one could easily get rid of iterations by using the axiom of choice but this would introduce into the construction an unpleasant element of uncontrollable arbitrariness.

In conclusion we consider the question of whether the universal covering is a functor.

A category AR-**C** is defined for any category **C**, whose objects are morphisms $\pi: \tilde{X} \to X$ of **C** and whose morphisms

are commutative diagrams of the form

$$
(4)\qquad
\begin{tikzcd}
\tilde{X} \arrow[r, "\tilde{f}"] \arrow[d, "\pi"'] & \tilde{Y} \arrow[d, "\rho"] \\
X \arrow[r, "f"'] & Y
\end{tikzcd}
$$

where $\tilde{f}$ and f are morphisms of $\mathbf{C}$. Morphism (4) is usually denoted by $(\tilde{f}, f)$ and assumed to be a morphism of an object $\pi\colon \tilde{X} \to X$ into an object $\rho\colon \tilde{Y} \to Y$. The composition of these morphisms can be defined in an obvious way.

In particular, when $\mathbf{C}$ = TOP and $\mathbf{C}$ = TOP$^\bullet$ we obtain categories AR-TOP and AR-TOP$^\bullet$. Complete subcategories of these categories whose objects are coverings will be denoted by COV and COV$^\bullet$ respectively and referred to as *categories of coverings*. Morphisms of these categories are squares of the form (4) in which π and ρ are coverings and $\tilde{f}$ and f are continuous mappings.

Morphisms in the sense of Definition 6 now to be referred to as *morphisms over* X are a special case of morphisms $(\tilde{f}, f)$ resulting when $f = \mathrm{id}$. This means that *for any (pointed) space X the category* COV (X) (*the category* COV$^\bullet$ (X)) *is a subcategory of the category* COV (*the category* COV$^\bullet$).

By associating a space X with every (pointed) covering $\pi\colon \tilde{X} \to X$ and a mapping f with every morphism $(\tilde{f}, f)$ we obviously obtain some functor COV $\to$ TOP (functor COV$^\bullet$ $\to$ TOP$^\bullet$). For any (pointed) space X the category COV (X) (category COV$^\bullet$ (X)) is obviously the inverse image of the trivial category (X, id_X) under that functor.

Let H-TOP$^\bullet$ be a complete subcategory of TOP$^\bullet$, composed of Hausdorff connected locally connected and semi-locally simply connected spaces and let H-COV$^\bullet$ be its inverse image under the functor COV$^\bullet$ $\to$ TOP$^\bullet$. In other words H-COV$^\bullet$ is a complete subcategory of the category of

pointed coverings $\mathrm{COV}^{\bullet}$ composed of coverings over a space in H-TOP.

Theorem 3. There is a functor

$$\text{(5)} \qquad \text{H-TOP}^{\bullet} \to \text{H-COV}^{\bullet}$$

associating with every pointed space (X, x_0) *of the category* $\text{H-TOP}^{\bullet}$ *some simply connected universal pointed covering of it*

$$\text{(6)} \qquad \pi_X\colon (\widetilde{X}, \widetilde{x}_0) \to (X, x_0).$$

This functor is unique to within an isomorphism.

Proof. We define functor (5) on the objects by choosing covering (6) arbitrarily for every space (X, x_0). Let f: $(X, x_0) \to (Y, y_0)$ be a pointed mapping. Since $\widetilde{X}$ is a simply connected space, by Theorem 1 there is a unique mapping $\widetilde{f}$: $(\widetilde{X}, \widetilde{x}_0) \to (\widetilde{Y}, \widetilde{y}_0)$ which is a lifting of the mapping $\pi_X \circ f$ with respect to a covering π_Y and which makes up therefore together with f a morphism $(\widetilde{f}, f)$ of π_X into π_Y. On associating the morphism $(\widetilde{f}, f)$ with the mapping f we just obtain ($\widetilde{f}$ being a unique mapping) the required functor (5).

Having chosen covering (6) in a different way we obtain an isomorphic functor (the fact that the isomorphism will be functorial again follows from uniqueness). □

Remark 1. The presented construction of functor (5) contains an unpleasant element of arbitrariness. Although that arbitrariness is harmless, leading as it does to naturally isomorphic functors, we can get rid of it, if desired, by taking the coamalgam of a complete family of coverings as coverings (6) from Lemma 6. (Notice that the corresponding construction uniquely defines not only the space $\widetilde{X}$ but also a base point $\widetilde{x}_0$.)

Lecture 9

Smooth coverings · Isomorphism of the categories of smooth and topological coverings · The existence of universal smooth coverings · The coverings of smooth and topological groups · Universal coverings of Lie groups · Lemmas on topological groups · Local isomorphisms and coverings · The description of locally isomorphic Lie groups

Let us apply the results obtained in Lecture 8 to smooth manifolds and to Lie groups. For a smooth (connected) manifold M we shall call the coverings $\widetilde{M} \to M$ in the sense of Definition 1, Lecture 8, i.e. coverings of M as a topological space, *topological coverings*, and denote the category of all such coverings by $\mathrm{COV_{top}}(M)$.

Definition 1. A covering $\pi: \widetilde{M} \to M$, where $\widetilde{M}$ and M are connected smooth manifolds, is said to be a *smooth covering* if it is a smooth mapping of $\widetilde{M}$ onto M and for any connected open set $U \subset M$ evenly covered by the mapping π a restriction of π to every component $\widetilde{U}$ of the set $\pi^{-1}(U)$ is a diffeomorphism $\widetilde{U} \to U$.

The last condition implies in particular that any smooth covering is étale (is a local diffeomorphism).

The trivial covering $\mathbb{R} \to \mathbb{R}$, $x \mapsto x^3$, is an example of a nonsmooth covering that is a smooth mapping.

We shall denote the category whose objects are smooth coverings of smooth manifolds and whose morphisms are their morphisms $(\tilde{f}, f)$ (consisting of smooth mappings $\tilde{f}$ and f) as topological coverings by the symbol COV-DIFF and denote its subcategory, which consists of the coverings of

a given manifold M and their morphisms over M, by the freed symbol COV (M). COV$^\bullet$-DIFF and COV$^\bullet$ (M) denote the pointed versions of these categories.

Ignoring smoothnesses gives us some functor

$$\text{COV}\ (M) \to \text{COV}_{\text{top}}\ (M) \tag{1}$$

for any smooth manifold M.

Proposition 1. *Functor* (1) *is an isomorphism of categories, i.e. is a bijective mapping on objects and morphisms.*

Proof. The statement that functor (1) is bijective on objects implies that for any topological covering $\pi\colon \tilde{M} \to M$ on $\tilde{M}$ there is a unique smoothness with respect to which π is a smooth covering. To prove this consider on M an arbitrary chart (U, h) such that the set U is connected and evenly covered by the mapping π. Let $\tilde{U}$ be a component of the set $\pi^{-1}(U)$ and $\tilde{h} = h \circ (\pi|_{\tilde{U}})$. The pair $(\tilde{U}, \tilde{h})$ is clearly a chart on $\tilde{M}$. If $(\tilde{V}, \tilde{k})$ is another chart of this kind, then, since on the set $\tilde{k}(\tilde{U} \cap \tilde{V}) = k(U \cap V)$ we have $\tilde{h} \circ \tilde{k}^{-1} = h \circ k^{-1}$, the charts $(\tilde{U}, \tilde{h})$ and $(\tilde{V}, \tilde{k})$ are compatible with each other. This shows that all possible charts of the form $(\tilde{U}, \tilde{h})$ make up an atlas on $\tilde{M}$. The mapping π in the corresponding smoothness on $\tilde{M}$, will obviously be a smooth covering. The uniqueness of that smoothness follows immediately from the fact that in any smoothness on $\tilde{M}$ with respect to which π is a smooth covering pairs $(\tilde{U}, \tilde{h})$ are smooth charts.

The statement that functor (1) is bijective on morphisms now implies that for any two smooth coverings $\pi_1\colon \tilde{M}_1 \to M$ and $\pi\colon \tilde{M} \to M$ every morphism $\tilde{f}\colon \tilde{M}_1 \to \tilde{M}$ of them as topological coverings is a smooth mapping. But this is obvious after what has been said above. Indeed, since $\tilde{f}$ is a covering (Lemma 3, Lecture 8), there exists on M an atlas of charts (U, h) evenly covered by a mapping π on M such that all the corresponding charts of the form $(\tilde{U}, \tilde{h})$ on $\tilde{M}$ are evenly covered by the mapping $\tilde{f}$. This means that

for any chart of the form $(\tilde{U}, \tilde{h})$ on $\tilde{M}_1$ there is a chart $(\tilde{U}_1, \tilde{h}_1)$ such that covers a chart (U, h) and such that f homeomorphically maps $\tilde{U}_1$ onto $\tilde{U}$. But then $\tilde{h}_1 = \tilde{h} \circ f$ and therefore in those charts $\tilde{f}$ is given by the identity (and hence smooth) mapping. Therefore $\tilde{f}$ is a smooth mapping. □

Remark 1. A similar forgetful functor

$$\text{COV-DIFF} \to \text{COV}$$

is not an isomorphism of categories. On objects that functor is neither surjective (because of the existence of non-locally flat topological spaces) nor injective (because of the possibility of introducing on the same topological manifold many different smoothnesses) and its image is not a complete subcategory of the category COV. We can only say (by way of a direct generalization concerning morphisms in the statement of Proposition 1) that if *for a morphism* $(\tilde{f}, f)$ *of a smooth covering* π_1: $\tilde{M}_1 \to M_1$ *into a smooth covering* π: $\tilde{M} \to M$ *the mapping* f *is smooth, then so is the mapping* $\tilde{f}$. Indeed, (cf. the proof of Proposition 1) for any two charts (U_1, h_1) and (U, h) of manifolds M_1 and M the mapping $\tilde{f}$ is given in the corresponding covering charts $(\tilde{U}_1, \tilde{h}_1)$ and $(\tilde{U}, \tilde{h})$ by the same (and therefore smooth) functions as the mapping f is in the charts (U_1, h_1) and (U, h) (it is here assumed of course that $\tilde{f}(\tilde{U}_1) \subset \tilde{U}$ and hence $f(U_1) \subset U$). □

Any smooth manifold being a locally flat topological space is locally connected. It turns out that, in addition, it is semilocally simply connected and even *locally simply connected*, i.e. it has a base composed of simply connected open sets. This is immediately results from the following lemma:

Lemma 1. *A unit cube* Q *of* $\mathbb{R}^n$ *(no matter whether it is open or closed) is a simply connected space.*

We first prove the following lemma:

Lemma 2. *If simply connected (and connected) spaces* X *and* Y *are Hausdorff and locally connected, then their product* $X \times Y$ *is also simply connected.*

Proof. Let $\pi: \tilde{Z} \to X \times Y$ be a covering of the space $X \times Y$. We must show that that covering is trivial, i.e. (Proposition 4, Lecture 8) that it has a section $\sigma: X \times Y \to \tilde{Z}$.

Let us choose (and fix) arbitrary points $x_0 \in X$, $y_0 \in Y$ and $\tilde{z}_0 \in \pi^{-1}(x_0, y_0)$. By Theorem 1 there is a unique mapping

$$\tau: (Y, y_0) - (\tilde{Z}, \tilde{z}_0)$$

which has the property such that $(\pi \circ \tau)(y) = (x_0, y)$ for any point $y \in Y$ (that mapping is nothing but a lifting of the mapping $y \mapsto (x_0, y)$ of a connected locally connected and simply connected pointed space (Y, y_0) into a Hausdorff pointed space $(X \times Y, (x_0, y_0))$). Similarly for any point $y \in Y$ there is a unique mapping

$$\sigma_y: (X, x_0) \to (\tilde{Z}, \tau(y))$$

which has the property such that

$$(\pi \circ \sigma_y)(x) = (x, y)$$

for every point $x \in X$. But then the mapping

$$\sigma: X \times Y \to \tilde{Z}$$

defined by the formula

$$\sigma(x, y) = \sigma_y(x), \ (x, y) \in X \times Y$$

will obviously satisfy the relation $\pi \circ \sigma = \mathrm{id}$. To complete the proof, therefore, it remains to show that σ is a continuous mapping.

To do this it suffices to show that the image $A = \sigma(X \times Y)$ of the space $X \times Y$ under mapping σ is an open subset of a space $\tilde{Z}$. Indeed, any point $\tilde{z} \in A$ will then have a neighbourhood W entirely contained in A, and the image $\pi(W)$ of that neighbourhood under mapping π will be a neighbourhood of a point $\pi(\tilde{z})$ mapped by means of σ onto W.

On choosing a point $y_1 \in Y$, consider a subset $\sigma_{y_1}(X)$ of the set $\tilde{Z}$ (known to be homeomorphic to the space X). Let B be the set of all interior points of the set A, that are in

the subset $\sigma_{y_1}(X)$. We must prove that $B = \sigma_{y_1}(X)$. Since B is open in $\sigma_{y_1}(X)$, it suffices to show that B is nonempty and closed in $\sigma_{y_1}(X)$.

Let $\tilde{z}_1 \in \sigma_y(X)$ and let $\pi(\tilde{z}_1) = (x_1, y_1)$. There are connected neighbourhoods U and V of points x_1 and y_1 in X and Y, such that $U \times V$ is evenly covered by the mapping π. Let W be a component of $\tilde{z}_1$ in $\pi^{-1}(U \times V)$. It is clear that

$$W = \bigcup_{y \in V} \tilde{U}(y),$$

where $\tilde{U}(y) = W \cap \pi^{-1}(U \times \{y\})$. Each of the sets $\tilde{U}(y)$ either does not intersect A or is entirely contained in A.

In the case where $x_1 = x_0$ the sets $\tilde{U}(y)$ are nothing but the intersections of the neighbourhood W and $\sigma_y(X)$:

$$\tilde{U}(y) = W \cap \sigma_y(X).$$

In that case therefore $\tilde{U}(y) \subset A$ and hence $W \subset A$. Since W is open in $\tilde{Z}$, this means that the point $\tilde{z}_1$ for which $x_1 = x_0$ is in B. Hence B is a nonempty set.

Now let $\tilde{z}_1$ be a point in the closure $\bar{B}$ of B. Then the set $\tilde{U}(y_1)$ (a neighbourhood of $\tilde{z}_1$ in $\sigma_{y_1}(X)$) intersects the set B. Let $\tilde{z}_2 \in B \cap \tilde{U}(y_1)$ and $\pi(\tilde{z}_2) = (x_2, y_2)$. Since $\tilde{z}_2$ is an interior point of the set A, there is a neighbourhood V' of a point y_1 in a space Y, such that $V' \subset V$ and the intersection $W \cap \pi^{-1}(\{x_2\} \times V')$ is contained in A. This means that for any point $y \in V'$ the set $\tilde{U}(y)$ intersects the set A. But then we necessarily have $\tilde{U}(y) \subset A$. Hence the set

$$W' = \bigcup_{y \in V'} \tilde{U}(y)$$

is contained in A. The set W' is obviously open in Z' and contains the point $\tilde{z}_1$. Therefore $\tilde{z}_1 \in B$. Hence the set B is closed. □

Now we can prove Lemma 1.

Proof of Lemma 1. By virtue of Lemma 2 it suffices to consider the case where Q is a one-dimensional cube, i.e.

it is an interval of the axis $\mathbb{R}$. Suppose first that the interval is closed. Then for any covering $\pi: \tilde{Q} \to Q$ there is a finite covering of the interval Q by evenly covered open (in Q) intervals $I_1, \ldots, I_n$. These can clearly be numbered sequentially, i.e. so that for any $k = 1, \ldots, n$ the union J_k of intervals $I_1, \ldots, I_k$ should be connected and hence be also an interval. The intersections $J_k \cap I_{k+1}$ will be connected, and therefore an $(n-1)$-fold application of Corollary 1 to Proposition 1 of the preceding lecture will show us that the interval $J_n = Q$ is evenly covered by the mapping π. Hence the mapping π is trivial, and therefore the interval Q is simply connected.

But the open interval Q is the union of an increasing sequence of closed intervals over each of which the covering π is trivial, i.e. a homeomorphism. Therefore π is a homeomorphism over the whole Q as well. Thus the open interval Q is also simply connected. $\square$

Corollary. *Given $n \geqslant 2$ the sphere S^n is simply connected.*

Proof. Let p and q be two antipodal points of the sphere S^n and let $U = S^n \setminus \{p\}$ and $V = S^n \setminus \{q\}$. The open sets U and V are homeomorphic to an open n-dimensional cube and are, therefore, simply connected. Their intersection $U \cap V = S^n \setminus (\{p\} \cup \{q\})$ is homeomorphic to the product $S^{n-1} \times (0, 1)$ of the equator S^{n-1} of the sphere S^n by an open interval $(0, 1)$ and is therefore connected (given $n - 1 \geqslant 1$). Hence by Corollary 2 to Theorem 1 of Lecture 8 the sphere $S^n = U \cup V$ is simply connected. $\square$

Let H-DIFF be a category of pointed smooth Hausdorff manifolds. By the foregoing the smoothness ignoring functor maps this category into the category H-TOP$^\bullet$. Combining this functor and the functor of Theorem 3 in the preceding lecture we associate a simply connected covering $\tilde{M} \to M$ with every manifold M. By Proposition 1 a smooth-covering structure is uniquely introduced into that covering. It is clear that we thus obtain some functor from the category H-DIFF$^\bullet$ to the category H-COV$^\bullet$ of pointed coverings over Hausdorff manifolds.

We state this fact as a separate theorem:

Theorem 1. *There is a functor*

$$\text{H-DIFF}^\bullet \to \text{H-COV}^\bullet$$

associating every pointed Hausdorff manifold M with its simply connected universal pointed covering

$$\pi_M : \widetilde{M} \to M.$$

That functor is unique to within an isomorphism. $\square$

We now proceed to Lie groups. The notion of covering is introduced by the following definition:

Definition 2. Let $\widetilde{G}$ and G be connected Lie groups. A smooth covering $\pi: \widetilde{G} \to G$ is said to be a *group covering* i it is a homomorphism of groups.

In a similar fashion we can introduce the notion of group covering for the case where $\widetilde{G}$ and G are connected topological groups.

Morphisms of group coverings are the morphisms $(\widetilde{f}, f)$ of them as smooth (or topological) coverings for which the mappings $\widetilde{f}$ and f are homomorphisms.

Since in every group we can single out in a natural manner a base point, its identity element, and since any homomorphism sends identity to identity, all group coverings and all their morphisms are clearly pointed.

All groups coverings of Lie groups (or of topological groups) and all their morphisms constitute the category COV-GR.

Any Lie group G defines a subcategory of COV-GR whose objects are the group coverings of the group G and whose morphisms are the morphisms of COV-GR of the form $(\widetilde{f}, \mathrm{id})$. We shall denote that subcategory, without fearing certain ambiguity, by COV (G) (and the category of coverings of the group G as smooth Hausdorff pointed manifold will be denoted by $\mathrm{COV}_{\mathrm{diff}}(G)$).

It turns out that like functor (1) the *forgetful functor*

$$\mathrm{COV}\,(G) \to \mathrm{COV}_{\mathrm{diff}}(G) \tag{2}$$

is an isomorphism of categories.

We shall prove this statement only partially.

For any group covering $\pi: \widetilde{G} \to G$ the mappings

$$\begin{aligned} &\widetilde{\mu}: \widetilde{G} \times \widetilde{G} \mapsto \widetilde{G}, \ (\widetilde{x}, \widetilde{y}) \mapsto \widetilde{x}\widetilde{y}, \\ &\widetilde{\nu}: \widetilde{G} \to \widetilde{G}, \quad \widetilde{x} \mapsto \widetilde{x}^{-1}, \end{aligned} \tag{3}$$

are liftings (with respect to π) of the mappings

$$\mu\colon \widetilde{G} \times \widetilde{G} \to G,\ (\widetilde{x},\ \widetilde{y}) \mapsto \pi\widetilde{x} \cdot \pi\widetilde{y},$$

$$\nu\colon \widetilde{G} \to G,\quad \widetilde{x} \to (\pi\widetilde{x})^{-1}.$$

Since these liftings are uniquely characterized (Proposition 3 of the preceding lecture) by the conditions

$$(4)\qquad \widetilde{\mu}\,(\widetilde{e},\ \widetilde{e}) = \widetilde{e},\quad \widetilde{\nu}\,(\widetilde{e}) = \widetilde{e},$$

where $\widetilde{e}$ is the identity of the group $\widetilde{G}$, functor (2) is an injective mapping on objects.

To prove that (2) is bijective, it is necessary to show for any pointed covering $\pi\colon (\widetilde{G}, \widetilde{e}) \to (G_{\text{diff}},\ e)$, where G_{diff} is the group G considered as a smooth manifold and e is its identity, that we can introduce a Lie-group structure into the manifold $\widetilde{G}$, with respect to which π will be a group covering. To do this one should clearly consider the mappings μ and ν (whose construction does not pressuppose that $\widetilde{G}$ is a group) and their liftings $\widetilde{\mu}$ and $\widetilde{\nu}$ that satisfy relations (4). *Suppose that liftings* $\widetilde{\mu}$ *and* $\widetilde{\nu}$ *exist.*

Since the mappings $\widetilde{\mu} = \pi \circ \widetilde{\mu}$ and $\nu = \pi \circ \widetilde{\nu}$ are smooth and π is a local diffeomorphism, the mappings $\widetilde{\mu}$ and $\widetilde{\nu}$ are also smooth. Moreover, it is clear that with respect to the operations

$$\widetilde{x}\widetilde{y} = \widetilde{\mu}\,(\widetilde{x},\ \widetilde{y}) \text{ and } \widetilde{x}^{-1} = \widetilde{\nu}\,(\widetilde{x})$$

the mapping π is a homomorphism. Therefore π will be a group covering if we show that those operations satisfy the group axioms.

Since $(\pi \circ \widetilde{\mu})\,(\widetilde{x},\ \widetilde{e}) = \pi\,(\widetilde{x})$ and $(\pi \circ \widetilde{\mu})\,(\widetilde{e},\ \widetilde{x}) = \pi\,(\widetilde{x})$, the mappings $\widetilde{x} \mapsto \widetilde{\mu}\,(\widetilde{e},\ \widetilde{x})$ and $\widetilde{x} \mapsto \widetilde{\mu}\,(\widetilde{x},\ \widetilde{e})$ are liftings of the mapping $\pi\colon \widetilde{G} \to G$, which have the property such that $\widetilde{e} \mapsto \widetilde{e}$. But the identity mapping id: $\widetilde{G} \to \widetilde{G}$ (which is also a lifting of the mapping π) has the same property. By the uniqueness of liftings, therefore, (Proposition 3 of Lecture 8)

we have equations $\tilde{\mu}(\tilde{x}, \tilde{e}) = \tilde{\mu}(\tilde{e}, \tilde{x}) = \tilde{x}$, i.e. equations $\tilde{x}\tilde{e} = \tilde{e}\tilde{x} = x$ which imply that the point $\tilde{e}$ is the identity of the multiplication μ.

In a similar fashion mappings $(\tilde{x}, \tilde{y}, \tilde{z}) \mapsto (\tilde{x}\tilde{y})\tilde{z}$ and $(\tilde{x}, \tilde{y}, \tilde{z}) \mapsto \tilde{x}(\tilde{y}\tilde{z})$ are liftings of the same mapping $(\tilde{x}, \tilde{y}, \tilde{z}) \mapsto \pi\tilde{x} \cdot \pi\tilde{y} \cdot \pi\tilde{z}$, both mappings sending the point $(\tilde{e}, \tilde{e}, \tilde{e})$ to the same point $\tilde{e}$. Therefore $(\tilde{x}\tilde{y})\tilde{z} = \tilde{x}(\tilde{y}\tilde{z})$ for any elements $\tilde{x}, \tilde{y}, \tilde{z} \in \tilde{G}$, so that the multiplication μ is associative.

Finally, the mapping $\tilde{x} \mapsto \tilde{x}\tilde{x}^{-1}$ is a continuous mapping of a connected space $\tilde{G}$ into a discrete space $\pi^{-1}(e)$ which sends $\tilde{e}$ to $\tilde{e}$. Therefore $\tilde{x}\tilde{x}^{-1} = \tilde{e}$ for any $\tilde{x} \in \tilde{G}$.

Consequently, G is a group. □

Thus the question of surjectivity of functor (2) on objects rests on the question of existence of liftings (3). We shall not prove their existence in full generality but restrict our discussion to the case where the *manifold* $\tilde{G}$ *is simply connected.*

In that case the existence of liftings $\tilde{\mu}$ and $\tilde{\nu}$ is ensured by Theorem 1 of the preceding lecture, since by Lemma 2, for a simply connected manifold $\tilde{G}$ the product $\tilde{G} \times \tilde{G}$ is also simply connected.

Thus we have proved the following proposition:

Proposition 2. *Let G be a Lie group and let $\pi: \tilde{G} \to \tilde{G}$ be a simply connected smooth covering of it as smooth pointed manifold. Then we can uniquely introduce into the smooth manifold $\tilde{G}$ a multiplication with respect to which it will be a Lie group and the mapping π will be a homomorphism (and hence a group covering).* □

As for the statement that functor (2) is bijective on morphisms, it is equivalent to the statement that for any two group coverings $\pi: \tilde{G} \to G$ and $\pi: \tilde{G}_1 \to G$ any morphism $\tilde{f}: \tilde{G} \to \tilde{G}_1$ of them as smooth coverings is a homomorphism $\tilde{G} \to \tilde{G}_1$. We shall prove even a more general result relating to coverings $\pi: \tilde{G} \to G$ and $\rho: \tilde{H} \to H$ of two, in general, distinct

Lie groups G and H and to a morphism $(\tilde{f}, f)$ of the category COV$^\bullet$-DIFF of covering π into covering ρ:

$$\begin{tikzcd}
\tilde{G} \arrow[r, "\pi"] \arrow[d, "\tilde{f}"'] & G \arrow[d, "f"] \\
\tilde{H} \arrow[r, "\rho"'] & H
\end{tikzcd}$$

It turns out that *if f is a homomorphism of groups, then so is $\tilde{f}$.* Indeed, mappings $\tilde{G} \times \tilde{G} \to \tilde{H}$ given by formulas $(\tilde{x}, \tilde{y}) \mapsto \tilde{f}(\tilde{x})\tilde{f}(\tilde{y})$ and $(\tilde{x}, \tilde{y}) \mapsto \tilde{f}(xy)$ both are liftings of the same mapping

$$(\tilde{x}, \tilde{y}) \mapsto f(x) f(y) = f(xy), \text{ where } x = \pi(\tilde{x}),\ y = \pi(\tilde{y}),$$

and therefore coincide. $\square$

It follows immediately that Theorem 1 remains also valid for Lie groups:

Theorem 2. *There is a functor* GR-DIFF $\to$ GR-DIFF *which associates every connected Lie group G with its simply connected group covering*

$$\pi_G : \tilde{G} \to G.$$

That functor is unique to within an isomorphism.

The kernel Ker π_G of the covering $\pi_G : \tilde{G} \to G$ is uniquely (to within an isomorphism) defined by the Lie group G. It is called the *fundamental group* (or *Poincaré group*) of that group and denoted by $\pi_1 G$. (It can be shown that $\pi_1 G$ coincides with the fundamental group $\pi_1 G_{\text{top}}$, known from topology, where G_{top} is a group G considered as a topological space, see [9].)

For applications we have in mind it is convenient to restate Theorem 2 in more algebraic terms. To do this we shall need several simple lemmas on topological groups.

Lemma 3. *Every open subgroup H of an arbitrary topological group G is closed.*

Proof. Since a subgroup H is open, so is every coset Hx of G mod H. Therefore the union of any family of these cosets is an open set. In particular, an open set is the union of all cosets Hx other than the subgroup H itself. But this union is the complement in G to the subgroup H. Therefore H is closed. □

Lemma 4. *Every neighbourhood V of the identity of a connected topological group G generates a group G.*

Proof. Let H be a subgroup generated by a neighbourhood V. Since $Vx \subset H$ for any $x \in H$, the subgroup H is open. But then by Lemma 3 H is also closed. Hence $H = G$, for under the hypothesis G is a connected group. □

Recall that for any invariant subgroup (normal divisor) K of the topological group G the factor group G/K is supipied with a *factor topology* in which the set $V \subset G/K$ is open If and only if so is its complete inverse image $\pi^{-1}(V)$ under the natural epimorphism $\pi: G \to G/K$ in G. With respect to that topology the factor group G/K is a topological group.

Lemma 5. *For any invariant subgroup $K \subset G$ the natural epimorphism $\pi: G \to G/K$ is an open mapping. For any open epimorphism $\Phi: G \to H$ the factor group G/K of a group G mod the kernel $K =$ Ker Φ of the epimorphism Φ is isomorphic to the group H. The isomorphism $\varphi: G/K \to H$ can be chosen so that we have a commutative diagram*

$$\begin{tikzcd} & G/K \arrow[d, "\varphi"] \\ G \arrow[ur, "\pi"] \arrow[r, "\Phi"'] & H \end{tikzcd} \tag{5}$$

Proof. If U is open in G, then the set UK, being the union of open sets Ux, $x \in K$, is also open in G. But clearly $UK = \pi^{-1}(\pi U)$. Hence the set πU is open in G/K. This proves the first statement.

It is clear that the formula $\varphi(xK) = \Phi(x)$ correctly defines the algebraic isomorphism $\varphi: G/K \to H$ for which diagram (5) is commutative. We only need to prove therefore that φ is a homeomorphism.

But if V is open in H, then $\Phi^{-1}(V)$ is open in G (for Φ is continuous), and since π is open, $\pi(\Phi^{-1}(V)) = \varphi^{-1}(V)$ is

13—0450

open in G/K. Similarly, if W is open in G/K, then $\pi^{-1}(W)$ is open in G, and since under the hypothesis Φ is open, $\Phi(\pi^{-1}(W)) = \varphi(W)$ is open in H. Hence φ is a homeomorphism. □

Definition 3. Let G and H be connected topological (or smooth) groups. A homomorphism $\Phi: G \to H$ of G into H is said to be a *local isomorphism* if Φ bijectively maps some neighbourhood U of the identity of G onto some neighbourhood V of the identity of H.

Since by Lemma 4 the group H is generated by V, every local isomorphism Φ is an epimorphism, and since that epimorphism, being a local diffeomorphism, is open, we can apply Lemma 5 to it. Therefore H is isomorphic to G/K, where $K = \operatorname{Ker}\Phi$. Under the hypothesis, $K \cap U = \{e\}$, which, by definition, means that the subgroup K is a *discrete subgroup* of G. Conversely, if K is a discrete invariant subgroup of G, then the natural epimorphism $\pi: G \to G/K$ is obviously a local isomorphism. By virtue of Lemma 5 this proves that the *local isomorphism $G \to H$ exists if and only if H is isomorphic to the factor group G/K of G mod some discrete invariant subgroup K.*

An example of a local isomorphism is obviously any group covering $G \to H$. Conversely, a local isomorphism $\Phi: G \to H$ is a group covering since it evenly covers V, a neighbourhood stipulated by Definition 3 (by virtue of Lemma 5 it may be assumed without loss of generality that $H = G/K$, where $K = \operatorname{Ker}\Phi$, and that Φ is a natural epimorphism $\pi: G \to G/K$, but then

$$\Phi^{-1}(V) = UK = \bigcup_{x \in K} Ux,$$

where the open sets $Ux \subset G$ do not intersect and each of them is homeomorphically mapped onto U), and hence evenly covers the neighbourhood Vh of an element $h \in H$. Thus *group coverings and local isomorphisms are the same thing.*

It is clear that the last statement holds for Lie groups as well. What is more it is easy to see that if we are given a group covering (= local isomorphism) $G \to H$, where H is a topological group and G is a Lie group, then a smoothness is introduced into H in a unique way with respect to which H is a Lie group and the mapping $G \to H$ is a smooth

covering. In particular, for any discrete invariant subgroup K of the Lie group G the factor group G/K thus turns out to be a Lie group, and therefore for any local isomorphism Φ: $G \to H$ of Lie groups the commutative diagram (5) is a diagram over the category of Lie groups.

All this implies that for Lie groups (as well as for topological groups) the following proposition is true:

Proposition 3. *A mapping Φ: $G \to H$ of connected groups is a group covering if and only if:*

(a) *it is a local isomorphism; or equivalently if*

(b) *there is a commutative diagram* (5), *where K is a discrete invariant subgroup, π is a natural epimorphism and φ is some isomorphism.* □

Of particular interest in connection with this proposition is the following, rather unexpected, lemma:

Lemma 6. *Every discrete invariant subgroup K of a connected topological (and, in particular, smooth) group G is in the centre of that group (and is, in particular, Abelian).*

Proof. Let $x \in K$ and let U be a neighbourhood of an element x containing no other elements of K. Consider a neighbourhood V of the identity of G which has the property such that $VxV^{-1} \subset U$. (That such a neighbourhood exists follows immediately from the fact that the mapping $y \to yxy^{-1}$ is continuous.) Since K is invariant and $U \cap K = \{e\}$, we have $yxy^{-1} = x$ for any element $y \in V$. This means that the *centralizer* of x (the subgroup of all elements commutative with x) contains the neighbourhood V. Hence, since V generates G, that centralizer coincides with G and therefore x is in the centre of G. □

Corollary. *The fundamental group $\pi_1 G$ of every connected Lie group G is an Abelian group.* □

Now we are ready to formulate our final theorem. In this theorem connected Lie groups G and H are said to be *locally isomorphic* if there are local isomorphisms of the form $P \to G$ and $P \to H$, where P is some connected Lie group.

Theorem 3. *For any connected Lie group G there is a simply connected Lie group $\tilde{G}$ isomorphic to it that depends functorially on G.*

$\tilde{G}$ is uniquely defined to within an isomorphism.

Two connected Lie groups G and H are locally isomorphic if and only if $\tilde{G}$ and $\tilde{H}$ are isomorphic.

A connected Lie group is locally isomorphic to a group G if and only if it is isomorphic to the factor group $\tilde{G}/K$ of $\tilde{G}$ mod a discrete (and therefore central) invariant subgroup K.

Proof. The first two statements are by virtue of Proposition 3 just a restatement of Theorem 2.

If $P \to G$ and $P \to H$ are local isomorphisms and $\tilde{P} \to P$ is a simply connected universal covering, then the composite mappings $\tilde{P} \to G$ and $\tilde{P} \to H$ are also universal coverings. Therefore $\tilde{P} \approx \tilde{G} \approx \tilde{H}$. Conversely, if $\tilde{G} \approx \tilde{H}$, then we have local isomorphisms $P \to G$ and $P \to H$, with $P = \tilde{G}$. This proves the third statement.

The fourth statement follows from the third by virtue of Proposition 3. □

In particular, it follows from Theorem 3 that the *relation of local isomorphism is an equivalence relation.*

The group $\tilde{G}$ is a *simply connected covering group* of the group G.

Lecture 10

Local isomorphisms and isomorphisms of localizations. The Cartan theorem. A final diagram of categories and functors. Reduction of the Cartan theorem. The globalizability of embeddable local groups. Reducing the Cartan theorem to the Ado theorem

---

Theorem 3 of Lecture 9 gives quite a satisfactory description of classes of locally isomorphic Lie groups but it has the disadvantage that these classes are not the classes that were introduced in Lecture 3, i.e. the classes of locally isomorphic Lie groups are classes of Lie groups isomorphic in the category of local groups GR-LOC. We therefore must prove in addition that both notions of local isomorphism coincide. The clue to this is the following proposition:

Proposition 1. *Let G and H be connected Lie groups, U a connected neighbourhood of the identity in G and $\varphi\colon U \to H$ be a smooth mapping such that $\varphi(xy) = \varphi(x)\varphi(y)$ for any elements $x, y \in U$ for which $xy \in U$. Then, if G is simply connected, there is a unique homomorphism $\Phi\colon G \to H$ extending φ, i.e. such that*

$$\Phi|_U = \varphi.$$

To prove this statement consider a subset D of $G \times G$ consisting of all pairs $(x_1, x_2) \in G \times G$ for which $x_1x_2^{-1} \in U$. The subset is obviously open and contains a diagonal $\Delta \subset G \times G$. Since D is the union of connected sets of the form $\{x\} \times Ux$, $x \in G$, each intersecting the diagonal Δ which is also a connected set (homeomorphic to G), the *set D is connected.*

A subset V of G is said to be *small* if $V \times V \subset D$. i.e. if $VV^{-1} \subset U$, and a subset W of the product $G \times H$ of the groups G and H is said to be *distinguished* if for any point $(x, y) \in W$ there is a small neighbourhood V of x in G such that

$$(v, \varphi(vx^{-1})\, y) \in W \text{ for any point } v \in V.$$

It is clear that:

(a) the empty set is distinguished;

(b) the entire product $G \times H$ is distinguished;

(c) the union of any family of distinguished sets is distinguished;

(d) the intersection of any finite family of distinguished sets is distinguished;

Distinguished sets therefore may be taken to be open sets of some new topology on $G \times H$. The product $G \times H$ provided with that topology is denoted by $\widetilde{X}$. Let

$$\pi\colon \widetilde{X} \to G$$

be a mapping defined by the formula

$$\pi(x, y) = x \qquad (x, y) \in \widetilde{X}.$$

It is clear that for any open set $V \subset G$ the set $\pi^{-1}(V)$ is distin guished and for any distinguished set $W \in X$ the set $\pi(W)$ is open. This means that π is a continuous and open mapping.

For any small open set $V \subset G$, any element $x_0 \in V$ and any element $y_0 \in H$ we denote the set of all pairs of the form $(x, \varphi(xx_0^{-1})\, y_0$, where $x \in V$ by $W(x_0, V, y_0)$. It is easily seen that the set $W(x_0, V, y_0)$ is distinguished. Indeed, if $(x, y) \in W(x_0, V, y_0)$, i.e. if $x \in V$ and $y = \varphi(xx_0^{-1})\, y_0$, then for any point $v \in V$ an equation

$$\varphi(vx^{-1})\, y = \varphi(vx^{-1})\, \varphi(xx_0^{-1})\, y_0 = \varphi(vx_0^{-1})\, y_0$$

holds which shows that $(v, \varphi(vx^{-1})\, y) \in W(x_0, V, y_0)$.

Clearly $(x_0, y_0) \in W(x_0, V, y_0)$, i.e. $W(x_0, V, y_0)$ is a neighbourhood of the point (x_0, y_0) in a space $\widetilde{X}$. It is obvious that π homeomorphically maps that neighbourhood onto the neighbourhood V. On the other hand, it is easily seen that the set $\pi^{-1}(V)$ is the union of all possible sets of

the form $W(x_0, V, y)$, where $x_0 \in W$ is fixed and $y \in H$ ranges over the whole of H, none of these sets intersects (if there is a point $(x, y) \in W(x_0, V, y_1) \cap W(x_0, V, y_2)$, then $\varphi(xx_0^{-1})\, y_1 = y = \varphi(xx_0^{-1})\, y_2$ and therefore $y_1 = y_2$).

It amounts to saying that every small open set $V \subset G$ is evenly covered by a mapping π. Since any element of G obviously has a small neighbourhood, this proves that the *mapping* π: $\widetilde{X} \to G$ *is a weak covering*. Therefore by Lemma 2 of Lecture 8 the *mapping*

$$\pi_0 = \pi|_{\widetilde{X}_0}: \widetilde{X}_0 \to G$$

is a covering for any component $\widetilde{X}_0$ of $\widetilde{X}$. We choose as $\widetilde{X}_0$ the component containing the point (e_G, e_H), where e_G and e_H are the identities of G and H respectively.

Now recall that under the hypothesis G is a simply connected group and therefore any covering of it is trivial, i.e. is a homeomorphism. In particular, the covering π_0 is a homeomorphism. The inverse homeomorphism π_0^{-1} sends every point $x \in G$ to some point in $\widetilde{X}_0$ of the form (x, y), where $y \in H$. Consequently, by putting $\Phi(x) = y$ we obtain some uniquely defined continuous mapping

$$\Phi: G \to H.$$

Thus for any point $x \in G$ the point $\Phi(x) \in H$ is uniquely characterized by the fact that $(x, \Phi(x)) \in \widetilde{X}_0$. Therefore, in particular, $\Phi(e_G) = e_H$.

Let D^* be a subset of D consisting of all the points $(x_1, x_2) \in D$ for which

$$\Phi(x_2) = \varphi(x_2 x_1^{-1})\, \Phi(x_1). \tag{1}$$

It is clear that $\Delta \subset D^*$, so that D^* is nonempty. In addition, it is easily seen that *for any small connected open set* $V \subset G$ *we have an inclusion*

$$V \times V \subset D^*.$$

Indeed, for any point $x_0 \in V$ the distinguished set $W(x_0, V, \Phi(x_0))$ is connected (since it is homeomorphic to V) and contains a point $(x_0, \Phi(x_0)) \in \widetilde{X}_0$. Therefore $W(x_0, V,$

$\Phi(x_0)) \subset \widetilde{X}_0$, i.e. for any point $x \in V$ the point $(x, \varphi(xx_0^{-1})\Phi(x_0))$ lies in $\widetilde{X}_0$. But according to the foregoing every point in $\widetilde{X}_0$ can be uniquely represented as $(x, \Phi(x))$. Therefore $\Phi(x) = \varphi(xx_0^{-1})\Phi(x_0)$, which is equivalent to the inclusion $(x_0, x) \in D^*$. Hence $V \times V \subset D^*$. □

Further, we can easily see that *if the product $V \times V'$ of two small connected open sets V and V' intersects D^*, then it is contained in D^**. Indeed, if $(x, x_0) \in D^*$, $(x_0, x_0') \in D^*$ and $(x_0', x') \in D^*$, then $(x, x') \in D^*$ (since $\Phi(x') = \varphi(x'x_0'^{-1})\Phi(x_0') = \varphi(xx'^{-1}_0)\varphi(x_0'x_0^{-1})\Phi'(x_0) = \varphi(x'x_0^{-1})\varphi(x_0x^{-1})\Phi(x) = \varphi(x'x^{-1})\Phi(x)$). On the other hand, if $(x_0, x_0') \in V \times V'$ and $(x, x') \in V \times V'$, then according to the foregoing $(x, x_0) \in D^*$ and $(x_0', x') \in D^*$. Therefore if in addition $(x_0, x_0') \in D^*$, then $(x, x') \in D^*$. □

Since sets of the form $V \times V'$ obviously constitute a base of the subspace D, it is immediate that the set D^* is open and closed in D. Since D is connected and D^* is nonempty, this is possible only when $D^* = D$. Thus, *equation* (1) *holds for any point* $(x_1, x_2) \in D$.

Now we are in a position to prove Proposition 1.

Proof of Proposition 1. That Φ is a unique homomorphism follows immediately from the fact that (see Lemma 3 of Lecture 9) the group G is generated by the neighbourhood U. We must only prove the existence of Φ, therefore.

We show that the required homomorphism is the mapping Φ constructed above.

By putting in (1) $x_1 = e_G$ and $x_2 = x$ we immediately get $\Phi(x) = \varphi(x)$ for any element $x \in U$. Proposition 1 therefore will be proved if we show that the mapping Φ is a homomorphism, i.e. that for any elements $x, x' \in G$

$$\Phi(x, x') = \Phi(x)\cdot\Phi(x'). \tag{2}$$

To this end we notice that with $x \in U$ equation (2) holds for any $x' \in G$ (since $(x', xx') \in D$ and therefore $\Phi(xx') = \varphi(x)\Phi(x') = \Phi(x)\Phi(x')$). On the other hand, since G is connected it is generated by a neighbourhood of the identity $U \cap U^{-1}$ and therefore every element $x \in G$ can be represented as

$$x = x_1x_2 \ldots x_n,$$

where $x_1, x_2, \ldots, x_n \in U$. Therefore by induction

$$\Phi(xx') = \Phi(x_1) \ldots \Phi(x_n)\,\Phi(x') \tag{3}$$

for any element $x' \in G$. In particular, with $x' = e_G$

$$\Phi(x) = \Phi(x_1) \ldots \Phi(x_n),$$

which in conjunction with (3) proves (2). □

The mapping φ appearing in Proposition 1 is nothing but a homomorphism of a local group G_{loc} into H_{loc}, where G_{loc} and H_{loc} are the images of groups G and H under the localization functor

$$\mathrm{GR}_0\text{-DIFF} \to \mathrm{GR\text{-}LOC} \tag{4}$$

and the mapping Φ is a homomorphism of G into H turning under functor (4) into a homomorphism φ. Hence Proposition 3 is nothing but the assertion that in the case where G is simply connected the condition of complete univalence of the functor (4) holds for groups G and H. If, therefore, we restrict ourselves to a complete subcategory GR_{00}-DIFF of the category GR_0-DIFF consisting of simply connected Lie groups, then that condition will be satisfied. Thus *on the category* GR_{00}-DIFF *the localization functor*

$$\mathrm{GR}_{00}\text{-DIFF} \to \mathrm{GR\text{-}LOC} \tag{5}$$

is completely univalent.

But it is easy to see that any completely univalent functor establishes a bijective correspondence between isomorphisms and therefore, in particular, sends only isomorphic objects to isomorphic. As applied to functor (5) this means that *simply connected Lie groups are isomorphic if and only if so are their localizations.*

This directly yields an affirmative answer to the question asked at the beginning of the lecture: *connected Lie groups are locally isomorphic in the sense of Lecture* 3 (*i.e. have isomorphic localizations*) *if and only if they are so in the sense of Theorem* 3 *of Lecture* 9. Indeed every local isomorphism in the sense of Definition 3 of Lecture 9 will obviously be an isomorphism of localization. Therefore, in particular, localizations of any Lie group G and of its universal covering

group $\widetilde{G}$ are isomorphic:

$$G_{\text{loc}} \approx \widetilde{G}_{\text{loc}}.$$

Hence if $G_{\text{loc}} \approx H_{\text{loc}}$, then $\widetilde{G}_{\text{loc}} \approx \widetilde{H}_{\text{loc}}$ and therefore, by the foregoing, $\widetilde{G} \approx \widetilde{H}$, so that G and H are isomorphic. $\square$

Thus *by the "local isomorphism" of Lie groups in Theorem* 3 *of Lecture* 9 *we mean the isomorphism of their localizations.*

This implies that the theorem gives a full answer to the question of invertibility of the localization functor (4):

$$G_{\text{loc}} \approx H_{\text{loc}} \textit{ if and only if } \widetilde{G} \approx \widetilde{H}.$$

In particular, *on the category* GR_{00}-DIFF *of simply connected Lie groups functor* (5) *is invertible* (to within an isomorphism).

This result cannot be considered to be full, however, since it remains unknown if every local Lie group is a localization of some Lie group, i.e. if functor (5) effects the equivalence of categories.

The answer to this question is yes:

Theorem 1 (Cartan). *Functor* (5) *effects the equivalence of the category* GR_{00}-DIFF *of connected simply connected Lie groups and the category* GR-LOC *of local Lie groups.*

Corollary. *The category of connected simply connected Lie groups is equivalent to the category of finite-dimensional Lie algebras over the field* $\mathbb{R}$. *The equivalence is effected by the Lie functor.*

This corollary is the acme of the theory we are developing. It allows us to reduce any question concerning connected and simply connected Lie groups to the corresponding problem of Lie algebras which, being a "linear" analogue of the original problem, is, as a rule, significantly simpler.

All the categories and functors we have considered constitute a commutative diagram

$$\begin{tikzcd}
 & \mathrm{GR}_{00}\text{-DIFF} \arrow[d] \arrow[dr] & \\
\mathrm{GR}_0\text{-DIFF} \arrow[ur, "2"] & \text{GR-LOC} \arrow[r] \arrow[dr] & \text{ALG-LIE} \\
\text{GR-DIFF} \arrow[u, "1"] \arrow[ur] & & \text{GRIE} \arrow[u]
\end{tikzcd}$$

Number 1 in this diagram designates the functor of going over to the component of the identity. It identifies groups that are extensions of a given connected Lie group by means of a discrete group. Number 2 designates the functor of going over to a universal covering group. It identifies groups that are factor groups of a given simply connected Lie group mod discrete (central) invariant subgroups.

The other arrows designate functors effecting the equivalence of categories.

The above diagram contains all the essential information about interrelations between Lie groups and Lie algebras.

Thus, to complete the entire theory it only remains to prove the Cartan theorem. The present state of affairs concerning this theorem turns out to be very peculiar, however, and may be said to be quite unsatisfactory.

The only way of proving the Cartan theorem is to construct some functor from the category of local groups (or equivalently Lie algebras) into the category of simply connected Lie groups, which would be quasi-inverse to the localization functor. Up to now, however, despite numerous attempts (at any rate much effort has gone into it here in Moscow) no explicit "natural" construction (a construction using only basic concepts) of such a functor has emerged and say Serre believes that no such construction exists (see [8] p. 259; notice at the same time that Serre calls the Cartan theorem "Lie's third theorem"). All known proofs (as a matter of fact, there are only two) of the Cartan theorem have no functorial (= natural) character and cause inward psychological protest. It is evident that the last word has not yet been said here. Those proofs of the Cartan theorem rely on the following category-theoretic lemma:

Lemma 1. *Let* A *and* B *be arbitrary categories and let* F: $\mathsf{A} \to \mathsf{B}$ *be a completely univalent functor from* A *to* B. *If for any object* B *of* B *there is an object* A *of* A *such that the object* FA *is isomorphic to* B, *then* F *is quasi-inverse* (*it effects the equivalence of categories*).

Proof. For every object B of B we choose arbitrarily and fix an object A of A that is provided by the hypothesis of the lemma and denote it by GB. Also we fix an isomorphism θ_B: $FGB \to B$. Since F is completely univalent, for any

morphism β: $B \to B_1$ there is one and only one morphism α: $GB \to GB_1$ for which there is a commutative diagram

$$\begin{tikzcd} FGB \arrow[r, "F\alpha"] \arrow[d, "\theta_B"'] & FGB_1 \arrow[d, "\theta_{B_1}"] \\ B \arrow[r, "\beta"'] & B_1 \end{tikzcd}$$

We set $\alpha = G\beta$.

It is immediate from the uniqueness of α that the constructed correspondences $B \mapsto GB$ and $\beta \mapsto G\beta$ constitute a functor G: $\mathsf{B} \to \mathsf{A}$, isomorphisms θ_B obviously constituting an isomorphism of the functor FG and the identity functor Id_B. In addition, for any object A of A the equation $F(\alpha_A) = \theta_{FA}$ defines some morphism α_A: $GFA \to A$ which is an isomorphism, with the isomorphisms α_A easily seen to constitute an isomorphism of the functor GF and the functor Id.

Hence the functor G is quasi-inverse to F. □

By virtue of this general lemma, for the Cartan theorem to be proved for any local Lie group it suffices to construct at least one Lie group, a neighbourhood of whose identity is that local group (or the local group isomorphic to it). It is possible (and that determines the success of the construction) not to take care of the functoriality and admit any arbitrariness in the construction.

Definition 1. We shall say that a local Lie group is *globalizable* if it is isomorphic to a localization of some Lie group (i.e. isomorphic to a neighbourhood of the identity of that group).

Thus to prove the Cartan theorem we must only establish that any local Lie group is globalizable.

Definition 2. A local Lie group K is said to be *embeddable* if it is a local subgroup of some Lie group G, i.e. more precisely, of the localization G_{loc} of that group.

The first step in our proof of the Cartan theorem is the following proposition:

Proposition 2. *Any embeddable local Lie group K is globalizable.*

Before proving this proposition we shall prove its analogue for topological groups.

Let G be a connected topological group and K a subspace of it containing the identity element e of G, such that $xy \in K$ and $x^{-1} \in K$ for any elements $x, y \in K \cap U_0$, where U_0 is some neighbourhood of G.

Lemma 2. *There is a topological group H and an injective homomorphism $i: H \to G$ homeomorphically mapping some neighbourhood V_0 of the identity of H onto some neighbourhood of the identity element e in a subspace K, i.e. onto a set of the form $K \cap U_{00}$, where U_{00} is a neighbourhood of e in G.*

Proof. We shall say that a subset $A \subset G$ *is separated from* e if there is a neighbourhood U of the point e in G, such that $A \cap U = \emptyset$. It is clear that if the *sets A and B are separated from e, then so is $A \cup B$.*

For any element $g \in G$ we shall denote by A^g the *set* $g^{-1}Ag$ of all elements of the form $g^{-1}ag$, $a \in A$. Obviously A^g *is separated from e if and only if A is separated from e.*

Now let H be the set of all elements $g \in G$ for which the symmetric difference

$$K^g \Delta K = (K^g \setminus K) \cup (K \setminus K^g) = (K^g \cup K) \setminus (K^g \cap K)$$

is separated from e. Since $K^{g^{-1}} \Delta K = (K^g \Delta K)^{g^{-1}}$ and $K^{g_1 g_2} \Delta K \subset (K^{g_1} \Delta K)^{g_2} \cup (K^{g_2} \Delta K)$, that set is a subgroup of G (or more precisely, of the corresponding abstract group G_{abstr}).

Let U_{00} be a neighbourhood of the identity e of G such that $xy \in U_0$ for any elements $x, y \in U_{00}$. Then $g^{-1}xg \in K$ and $gxg^{-1} \in K$ for any element $x, g \in K \cap U_{00}$. Therefore if $g \in K \cap U_{00}$, $y \in K^g \cap U_{00}^g$ and hence $x = gyg^{-1} \in K \cap U_{00}$, then $y = g^{-1}xg \in K$. Consequently $K^g \cap U_{00}^g \subset K \cap U_{00}$ and therefore $K^g \cap V_0 \subset K \cap V_0$, where $V_0 = U_{00} \cap U_{00}^g$. Conversely, if $x \in K \cap U_{00}$, then $y = gxg^{-1} \in K$ and hence $x = g^{-1}yg \in K^g$. Consequently $K \cap U_{00} \subset K^g \cap U_{00}$ and therefore $K \cap V_0 \subset K^g \cap V_0$. Thus $K \cap V_0 = K^g \cap V_0$, i.e. $(K^g \Delta K) \cap V_0 = \emptyset$. This proves that *for any element $g \in K \cap U_{00}$ the set $K^g \Delta K$ is separated from e*, i.e. that $g \in H$. Consequently $K \cap U_{00} \subset H$.

We introduce into H a topology by taking as neighbourhoods of the identity all possible sets of the form $V = K \cap U$, where $U \subset U_{00}$ is a neighbourhood of e in G

contained in U_{00}. An automatic check shows that this does introduce in H a topology with respect to which H is a topological group. The embedding i: $H \to G$ is an injective homomorphism of topological groups and on the neighbourhood $V_0 = K \cap U_{00}$ that mapping is a homeomorphism.

This completes the proof of Lemma 1. □

Notice that in general H *is not* a subgroup of G i.e. the mapping i: $H \to G$ is not a homeomorphism on $i(H)$. For example, if $K = \{e\}$, then H is a group G in a discrete topology.

Now we are ready to prove Proposition 2.

Proof of Proposition 2. Let the local group K be a local subgroup of a Lie group G and hence (see Lecture 7) let there be a chart $(U_0, h) = (U_0, x^1, \ldots, x^n)$ in G, such that $K \cap U_0$ is defined by the equations

$$x^{m+1} = 0, \ldots, x^n = 0.$$

Considering G as a topological group we can apply Lemma 2 to K. Thus by this lemma there is a topological group H and an injective continuous homomorphism i: $H \to G$ mapping homeomorphically some neighbourhood V_0 of the identity of H onto the set $K \cap U_{00}$, where U_{00} is a neighbourhood of the identity in G. We may assume without loss of generally that $U_{00} = U_0$.

Then the pair $(V_0, k) = (V_0, y^1, \ldots, y^m)$, where $y^j(v) = x^j(iv)$, $j = 1, \ldots, n$, is obviously some chart on H containing the element $e \in V$ and therefore for any element $a \in H$ the $(aV_0, k \circ L_{a^{-1}})$ is a chart on H containing an element a. If $aV_0 \cap bV_0 \neq \varnothing$, then on $(k \circ L_{a^{-1}})(aV_0 \cap bV_0) \subset \mathbb{R}^m$ the mapping $(k \circ L_{b^{-1}}) \circ (k \circ L_{a^{-1}})^{-1} = k \circ L_{b^{-1}a} \circ k^{-1}$ is (since $\mathbb{R}^m \subset \mathbb{R}^n$) a restriction of a smooth mapping $h \circ L_{i(b^{-1}a)} \circ h^{-1}$ and hence is itself a smooth mapping. This proves that all charts of the form $(aV_0, k \circ L_{a^{-1}})$ are compatible with one another and therefore make up some atlas on H. A direct check shows that with respect to the smoothness defined by that atlas the group H is a Lie group and the mapping i is a smooth homomorphism diffeomorphically mapping a neighbourhood V_0 onto $K \cap U_0$. Thus $H_{\mathrm{loc}} \approx K$, so that K is a globalizable local group. □

Lecture 11

Submanifolds of smooth manifolds · Subgroups of Lie groups · Integral manifolds of integrable subfiberings · Maximal integral manifolds · The idea of the proof of Theorem 1 · The local structure of submanifolds · The uniqueness of the structure of a locally rectifiable submanifold with a countable base · Submanifolds of manifolds with a countable base · Connected Lie groups have a countable base · The local rectifiability of maximal integral manifolds · The proof of Theorem 1

A two-dimensional torus T^2 may be thought of as a factor group of an additive group of the space $\mathbb{R}^2$ mod its lattice $\mathbb{Z}^2$, which consists of points with integral coordinates. Therefore any straight line in $\mathbb{R}^2$ passing through the point (0, 0) yields some subgroups in T^2. If the slope of the straight line in $\mathbb{R}^2$ is rational (and equals, say, m/n), then its image in T^2 is a circle running around the torus m times along a meridian and n times along a parallel. If, however, that slope is irrational, then the corresponding subgroup in T^2 (called the *irrational solenoid group*) is everywhere dense in T^2 and in the induced topology every neighbourhood of any point of it contains a neighbourhood that is a disjoint union of a countable number of intervals. Hence this subgroup is not a manifold.

This example explains why we accept the following, seemingly unnecessarily, general definition:

Definition 1. A smooth manifold N is said to be a *submanifold* of a smooth manifold M if:

(a) any point of N is in M, so that an embedding $\iota\colon N \to M$ is defined;

(b) ι: $N \to M$ is smooth (and therefore, in particular, continuous);

(c) at every point $a \in N$ the differential $(d\iota)_a$: $\mathsf{T}_a(N) \to \mathsf{T}_a(M)$ of ι is a monomorphism.

It is usual to identify every vector $A \in \mathsf{T}_a(N)$ with the vector $(d\iota)_a A$, i.e. to consider $\mathsf{T}_a(N)$ to be a subspace of the space $\mathsf{T}_a(M)$.

Any open submanifold is clearly a submanifold in terms of Definition 1. Such a submanifold is a subspace, i.e. the embedding ι is a homeomorphism onto its image. However, this is no longer the case, say, for the irrational solenoid group.

Definition 2. A Lie group H is said to be a *subgroup* of a Lie group G if the manifold H_{diff} is a submanifold of the manifold G_{diff} and the group H_{abstr} is a subgroup of the group G_{abstr}. The subgroup H of G is said to be an *invariant subgroup* if H_{abstr} is invariant.

In particular, irrational solenoids are its subgroups.

Let $\mathfrak{g} = \mathfrak{l}(G)$ and $\mathfrak{h} = \mathfrak{l}(H)$ be the Lie algebras of Lie groups G and H. If H is a subgroup of G, then the homeomorphism $\mathfrak{l}(\iota)$: $\mathfrak{h} \to \mathfrak{g}$ identified with the mapping $d(\iota)_e$: $\mathsf{T}_e(H) \to \mathsf{T}_e(G)$ is a monomorphism. It is usual to identify a Lie algebra $\mathfrak{h}$ with its image in $\mathfrak{g}$ under that monomorphism. Thus by virtue of this identification *the Lie algebras of subgroups of a Lie group G are subalgebras of the Lie algebra $\mathfrak{g}$ of G.* The correspondence $H \mapsto \mathfrak{h}$ between subgroups $H \subset G$ and subalgebras $\mathfrak{h} \subset \mathfrak{g}$ will be called a *Lie correspondence.* Since the Lie algebras of a group and components of its identity coincide, it is natural to consider only connected subgroups H. It turns out that if restricted to connected subgroups the Lie correspondence is bijective. Thus we have the following theorem:

Theorem 1. *The Lie correspondence $H \mapsto \mathfrak{h}$ is a bijective correspondence between connected subgroups of a Lie group G and subalgebras of a Lie algebra $\mathfrak{g} = \mathfrak{l}(G)$.*

The group G in this theorem may be considered to be connected, of course.

We shall prove Theorem 1 starting somewhat from afar.

Let M be a smooth manifold and let E be an integrable subfibering of a tangent boundle $\mathsf{T}(M)$ (see Lecture 7).

Definition 3. A submanifold N of M is said to be an *integral manifold* of E if the embedding $\iota\colon N \to M$ is integral with respect to E, i.e. if

$$E_a = \mathsf{T}_a(N)$$

for any point $a \in N$.

It is easy to see that E *is integrable* (*in the sense of Definition* 10 *of Lecture* 7) *if and only if at least one integral manifold of E passes through any point a of M.* Indeed this condition is clearly sufficient for integrability. Conversely, let E be integrable. Then it is completely integrable as well (the corollary to Proposition 6 of Lecture 7), i.e. (see Definition 13 of Lecture 7) M has an atlas consisting of charts $(U, x^1, \ldots, x^n)$ such that for any point $a \in U$ vectors $\left(\frac{\partial}{\partial x^1}\right)_a, \ldots, \left(\frac{\partial}{\partial x^m}\right)_a$ constitute a basis of a space E_a. For every point $\xi = (\xi^1, \ldots, \xi^{n-m}) \in \mathbb{R}^{n-m}$ we denote by V_ξ a set of points $a \in U$ whose coordinates satisfy the conditions

$$x^{m+1} = \xi^1, \ldots, x^n = \xi^{n-m}.$$

That set (if nonempty) is naturally provided with the structure of a smooth manifold which is diffeomorphic to some open set in $\mathbb{R}^m$. Clearly, the manifold is a submanifold in U (and hence in M), the subspace $\mathsf{T}_a(V_\xi)$ spanning at any point $a \in V_\xi$ the vectors $\left(\frac{\partial}{\partial x^1}\right)_a, \ldots, \left(\frac{\partial}{\partial x^m}\right)_a$. Consequently $\mathsf{T}_a(V_\xi) = E_a$, so V_ξ is an integral manifold of E. To complete the proof it remains to notice that for any point $a \in U$ the submanifold V_ξ, with $\xi = (x^{m+1}(a), \ldots, x^n(a))$ contains a. $\square$

Submanifolds of the form V_ξ will occur rather frequently in what follows. They will be referred to as *flat submanifolds* of a chart U.

We shall say that submanifolds N_1 and N_2 of M having a point $a \in M$ in common *locally coincide at a* if there is a submanifold N_0, open both in N_1 and N_2, such that $a \in N_0$.

It is easy to see that *any two integral manifolds N_1 and N_2 of an integrable subfibering E that pass through a point a locally coincide at a.* Indeed, let $\iota_1\colon N_1 \to M$ and $\iota_2\colon N_2 \to M$ be embeddings. By Lemma 2 of Lecture 7 there are neigh-

bourhoods V_1 and V_2 of a in N_1 and N_2 and a diffeomorphism $\beta\colon V_2 \to V_1$ such that $\iota_2 = \iota_1 \circ \beta$ on V_1. But since ι_1 and ι_2 are restrictions of the identity mapping $M \to M$, the equation $\iota_2 = \iota_1 \circ \beta$ is possible only when $\beta = \mathrm{id}$ (and hence $V_1 = V_2$). This completes the proof, since the equation $\iota_1 = \iota_2$ in some neighbourhood of a precisely means that N_1 and N_2 locally coincide at a. $\square$

For an integrable vector bundle E, consider the collection $\mathfrak{R}$ of all its integrable manifolds. According to the foregoing, if two submanifolds $N_1, N_2 \in \mathfrak{R}$ intersect, then for any point $a \in N_1 \cap N_2$, there is a submanifold N_0 such that $a \in N_0 \subset N_1 \cap N_2$ and N_0 is open both in N_1 and N_2. Since $N_0 \in \mathfrak{R}$ (an open submanifold of a manifold of $\mathfrak{R}$ is obviously in $\mathfrak{R}$), the family $\mathfrak{R}$ can be taken as a base of some new topology on M (whose open sets are the unions of submanifolds in $\mathfrak{R}$). A manifold M provided with this topology is denoted by M_E.

It is easy to see that the *identity mapping* $M_E \to M$ *is continuous*, i.e. any open set $U \subset M$ is open in M_E too. Indeed, let $a \in U$ and let $a \in N \in \mathfrak{R}$. Since N is locally connected, the component N_0 of the set $N \cap U$, which contains a point a, is open in N, i.e. is an open submanifold of N. Therefore $N_0 \in \mathfrak{R}$. This shows that U is the union of manifolds of $\mathfrak{R}$ and is therefore open in M_E. $\square$

Further, it is easy to see that the topology of the space M_E induces on any manifold $N \in \mathfrak{R}$ (which is by definition an open subset of M_E) the original topology of N, so that in other words *every integral manifold* $N \in \mathfrak{R}$ *is an open subspace of* M_E. Indeed any neighbourhood of a point $a \in N$ in the topology of N is an integral manifold in $\mathfrak{R}$ and hence an open set in M_E. Conversely, any neighbourhood U of a in the topology induced by that of M_E contains an integral manifold $N_1 \in \mathfrak{R}$ such that $a \in N_1$. Since N and N_1 locally coincide at a, there is a manifold $N_0 \in \mathfrak{R}$ containing a point a that is an open submanifold of both N and N_1. The manifold N_0 is the neighbourhood of a in the topology of N contained in U. Thus the original topology of N coincides with that induced on N by the topology of M_E. $\square$

Now let W be a component of connectedness of M_E (provided with an induced topology). Then for any point $a \in W$, every connected integral manifold N containing that point is

contained in W (for N is connected also as a subspace in M_E).

In particular, contained in W is a coordinate neighbourhood U of a in N. Since U, being an integral manifold, is open in M_E, it is a neighbourhood of a in W too. This allows every chart (U, h) at a on N to be considered as a chart on W too. Thus we obviously obtain on W some smoothness compatible with the topology.

The constructed smooth manifold W will obviously be a connected integral manifold of a subfibering E that contains a point a and has the property that any connected integral manifold of E containing the point a is contained in W and is open in W.

Definition 4. An integral manifold of a subfibering E is said to be *maximal* if it is connected and is not contained in any other connected integral manifold of that subfibering.

In particular, we see that the constructed integral manifold W is maximal.

This proves the following proposition:

Proposition 1. *Only one maximal integral manifold W of an integrable subfibering E passes through any point $a \in M$. Any connected integral manifold of E passing through a is open submanifold of W.* $\square$

To return to Lie groups, consider a subalgebra $\mathfrak{h}$ of the Lie algebra $\mathfrak{g}$ of a connected Lie group G. Recall that $\mathfrak{a}(G)$ denotes the infinite-dimensional Lie algebra of all vector fields on G. It is a module over the algebra $\mathcal{F}(G)$ of all smooth functions on G. For any subfibering $E \subset \mathsf{T}(G)$ the vector fields in E form a submodule $\mathfrak{a}(E)$ of the module $\mathfrak{a}(G)$. At the same time the Lie algebra $\mathfrak{g}$ and hence the Lie algebra $\mathfrak{l}$ are subalgebras in $\mathfrak{a}(G)$. Therefore the submodule $\mathcal{F}(G)\,\mathfrak{h}$ generated by $\mathfrak{h}$ is a subalgebra of $\mathfrak{a}(G)$, with $\mathcal{F}(G)\mathfrak{g} = \mathfrak{a}(G)$.

As a first step in the proof of Theorem 1 we show that *for any subalgebra $\mathfrak{h}$ of the Lie algebra $\mathfrak{g}$, there is a subfibering $E^{\mathfrak{h}}$ of a tangent bundle $\mathsf{T}(G)$ such that*

$$\mathfrak{a}(E^{\mathfrak{h}}) = \mathcal{F}(G)\,\mathfrak{h}. \tag{1}$$

Indeed, let $E_a^{\mathfrak{h}}$ be a subspace of a space $\mathsf{T}_a(G)$ consisting of vectors of the form X_a, where $X \in \mathfrak{h}$ (here we use the interpretation of $\mathfrak{g}$ as an algebra of left-invariant vector

fields; in the interpretation $\mathfrak{g} = \mathsf{T}_e(G)$ the subspace $E_a^{\mathfrak{h}}$ is the image of the space $\mathfrak{h} \subset \mathsf{T}_e(G)$ under the mapping $(dL_a)_e)$. It is easy to show that the union

$$E^{\mathfrak{h}} = \bigcup_{a \in G} E_a^{\mathfrak{h}}$$

of those subspaces is a subfibering of the bundle $\mathsf{T}(G)$ that has property (1). □

We shall say that the subfibering $E^{\mathfrak{h}}$ *is generated* by a subalgebra $\mathfrak{h}$.

According to the foregoing, it follows from (1) that $\mathfrak{a}(E^{\mathfrak{h}})$ is a subalgebra of $\mathfrak{a}(G)$, i.e. that $E^{\mathfrak{h}}$ is involutory. Consequently, by the Frobenius theorem (Proposition 5 of Lecture 7) the *subfibering* $E^{\mathfrak{h}}$ *is integrable.*

If a subalgebra $\mathfrak{h}$ is the Lie algebra of a connected subgroup H, then H is obviously an integral manifold of $E^{\mathfrak{h}}$ passing through the point e (a maximal manifold, as we shall see below). For any subalgebra $\mathfrak{h}$ therefore it is natural to consider a maximal integral manifold H of $E^{\mathfrak{h}}$ and to try to prove that it is a Lie subgroup having a Lie algebra $\mathfrak{h}$.

To do this it is in the first place necessary to prove that H_{abstr} *is a subgroup of a group* G_{abstr}, i.e. that $xy \in H$ and $x^{-1} \in H$ for any elements $x, y \in H$. This is easy to do using the following general considerations.

Let $\Phi\colon M \to M'$ be a diffeomorphism and let N be a submanifold of M. Consider the image N' of N under Φ. Since Φ bijectively maps N onto N', we can use Φ to transfer the smoothness from N to N'. Thus N' will turn out to be a smooth manifold and Φ will induce some diffeomorphism $\Phi_N\colon N \to N'$ that closes the commutative diagram

$$\begin{tikzcd}
N \arrow[r, "\Phi_N"] \arrow[d, "\iota"'] & N' \arrow[d, "\iota'"] \\
M \arrow[r, "\Phi"'] & M
\end{tikzcd}$$

in which the vertical arrows are embeddings. The commutativity of this diagram implies that $\iota' = \Phi \circ \iota \circ \Phi_N^{-1}$, from which it is immediate that the mapping ι' is smooth and that its differential $(d\iota')_{a'}$ at every point $a' \in N'$ is a monomorphism. This means that *N' is a submanifold of M.* We shall refer to that submanifold as the *image* of N under the diffeomorphism Φ.

If now E is an integrable subfibering of the bundle $\mathsf{T}(M)$, then its image E' under the diffeomorphism $\mathsf{T}(\Phi)$: $\mathsf{T}(M) \to \mathsf{T}(M')$ is an integrable subfibering of $\mathsf{T}(M')$ and the *image of any maximal integral manifold of E under Φ is a maximal integral manifold of the subfibering E'.*

Since for $M = M' = G$, $E = E^{\mathfrak{h}}$ and $\Phi = L_x$ (or $\Phi = I$, where I: $G \to G$ is a mapping $x \mapsto x^{-1}$) the subfibering E' coincides obviously with $E = E^{\mathfrak{h}}$, it follows that the diffeomorphism Φ sends the maximal integral submanifold H of $E^{\mathfrak{h}}$ passing through the point e to the maximal integral submanifold passing through a point Φe, i.e. to the same H when $\Phi e \in H$. Since for $\Phi = I$, as well as for $\Phi = L_x$, $x \in H$, the condition $\Phi e \in H$ obviously holds, this proves that $I(H) = H$ and $L_x(H) = H$ for $x \in H$, i.e. that *H is a subgroup.*

To complete the proof it remains to show that H is a Lie group, i.e. that $(x, y) \mapsto xy$ and $x \mapsto x^{-1}$ are smooth mappings. As regards $x \mapsto x^{-1}$ this fact follows from the foregoing, but as for $(x, y) \mapsto xy$, we may only say that this mapping is smooth only in x or in y separately.

It turns out unexpectedly that a complete proof of the smoothness of $(x, y) \mapsto xy$ is quite a difficult task involving subtle topological phenomena and requiring much preliminary work. Therefore we shall have to return to the fundamentals of the theory.

Definition 5. The *rank* of a smooth mapping Φ: $N \to M$ at a point $a \in N$ is the rank of its differential

$$(d\Phi)_a\colon \mathsf{T}_a(N) \to \mathsf{T}_a(M)$$

considered as the linear mapping of vector space $\mathsf{T}_a(N)$ into vector space $\mathsf{T}_a(M)$.

Let $y^1, \ldots, y^m$ be local coordinates on N at a and let $x^1, \ldots, x^n$ be local coordinates of M at Φa. Further,

let

$$\varphi^1(y), \ldots, \quad \varphi^n(y), \quad y = (y^1, \ldots, y^n),$$

be functions expressing the mapping Φ in terms of those coordinates. Since the matrix of the linear mapping $(d\Phi)_a$ in the bases $\left(\frac{\partial}{\partial y^1}\right)_a, \ldots, \left(\frac{\partial}{\partial y^m}\right)_a$ and $\left(\frac{\partial}{\partial x^1}\right)_{\Phi a}, \ldots, \left(\frac{\partial}{\partial x^n}\right)_{\Phi a}$ is the Jacobian matrix whose elements are partial derivatives

$$(2) \qquad \left(\frac{\partial \varphi^i}{\partial y^j}\right)_a, \quad i = 1, \ldots, n, \quad j = 1, \ldots, m,$$

calculated at a point $(y^1(a), \ldots, y^m(a)) \in \mathbb{R}^m$, the *rank of Φ at a equals the rank of the matrix with elements* (2).

It follows from continuity that the rank r' of Φ at any point a' of some neighbourhood of a is at least its rank r at a:

$$r' \geqslant r.$$

If $r' = r$ for any point $a' \in U$, then Φ is said to be *locally flat* at a.

It may be assumed, after rewriting the coordinates if necessary, that

$$(3) \qquad \det\left|\left(\frac{\partial \varphi^i}{\partial y^j}\right)_a\right| \neq 0 \text{ for } i, j = 1, \ldots, r.$$

Consider the functions $y'^1, \ldots, y'^m$ defined in a neighbourhood of a by the formulas

$$y'^j(y^1, \ldots, y^m) = \begin{cases} \varphi^j(y^1, \ldots, y^m) & \text{if } 1 \leqslant j \leqslant r, \\ y^j, & \text{if } r+1 \leqslant j \leqslant m. \end{cases}$$

Since by condition (3) the Jacobian $\frac{D(y'^1, \ldots, y'^m)}{D(y', \ldots, y^m)}$ at a is nonzero, the functions $y'^1, \ldots, y'^m$ are local coordinates in some neighbourhood of a. In these coordinates the mapping Φ can be expressed as

$$x^i = \begin{cases} y'^i, & \text{if } 1 \leqslant i \leqslant r, \\ \varphi'^i(y'^1, \ldots, y'^m), & \text{if } r+1 \leqslant i \leqslant n. \end{cases}$$

If Φ is locally flat at a, then in these formulas the functions $\varphi'^i(y'^1, \ldots, y'^m)$, $r + 1 \leqslant i \leqslant n$, are easily seen

to be independent of the coordinates $y'^{r+1}, \ldots, y'^{m}$, i.e. are of the form

$$\varphi'^{r+1}(y'^1, \ldots, y'^r), \ldots, \quad \varphi'^n(y'^1, \ldots, y'^r).$$

Therefore the formulas

$$x'^i = \begin{cases} x^i, & \text{if } 1 \leqslant i \leqslant r, \\ x^i - \varphi'^i(x^1, \ldots, x^r), & \text{if } r+1 \leqslant i \leqslant n, \end{cases}$$

define in some neighbourhood of Φa local coordinates $x'^1, \ldots, x'^n$ having the property that in coordinates $y'^1, \ldots, y'^n$ and $x'^1, \ldots, x'^n$ the mapping Φ can be manifested as

$$x'^i = \begin{cases} y'^i, & \text{if } 1 \leqslant i \leqslant r, \\ 0, & \text{if } r+1 \leqslant i \leqslant n. \end{cases}$$

The following proposition has thus been proved.

Proposition 2. *If a smooth manifold Φ: $N \to M$ is locally flat at a point $a \in N$ and has at that point a rank r, then on the manifolds N and M there are local coordinates $y^1, \ldots, y^m$ and $x^1, \ldots, x^n$ (defined in the neighbourhoods of a and Φa respectively) such that*

$$x^i \circ \Phi = \begin{cases} y^i, & \text{if } 1 \leqslant i \leqslant r, \\ 0, & \text{if } r+1 \leqslant i \leqslant n. \quad \square \end{cases}$$

As applied to an embedding ι: $N \to M$ of a manifold N into M (which is obviously a locally flat mapping) this proposition says that *for any point $a \in N$ in M there is a chart $(U, x^1, \ldots, x^n)$ with $a \in U$, such that the functions*

$$x^1 \circ \iota, \ldots, \quad x^m \circ \iota \tag{4}$$

are local coordinates in some neighbourhood V of a on V and the functions

$$x^{m+1} \circ \iota, \ldots, x^m \circ \iota$$

are identically zero (in V).

The last statement implies that the *submanifold N locally coincides at a with the flat submanifold $V_0 = V$ of U.*

Remark 1. The example of an irrational solenoid shows that in general $V_0 \neq U \cap N$.

Since the embedding ι: $N \to M$ is smooth, for any function f smooth in M its restriction $f \circ \iota$ to N is smooth in N

(of course, if that restriction exists, i.e. the domain $W(f)$ of f intersects with N). Conversely, consider a function g smooth in N. Let the domain $W(g)$ of the function contain the above coordinate neighbourhood V of a on N. Then

$$g = \hat{g}(x^1 \circ \iota, \ldots, x^m \circ \iota) \text{ on } V,$$

where $\hat{g}$ is some smooth function of m variables. We define in the coordinate neighbourhood U of the point a on M a function f using the formula

$$f = \hat{g}(x^1, \ldots, x^m).$$

Clearly f is a smooth function and $f \circ \iota = g$. We have thus proved the following lemma:

Lemma 1. *Any point of a submanifold N has a neighbourhood V such that every function smooth in N is a restriction to V of some function smooth in M.* □

Corollary. *If there is a submanifold structure on some subset N of a smooth manifold M, then for a given topology on N that structure is unique, i.e. any other submanifold structure on N will induce another topology on N.*

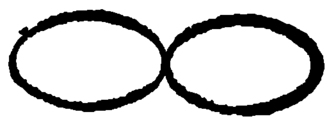
Proof. By virtue of Lemma 1 every smooth chart $(W, y^1, \ldots, y^m)$ on N consists of an open set W and functions $y^1, \ldots, y^m$ with a nonzero Jacobian which are locally restrictions to N of functions smooth in M. Therefore any two submanifold structures on N inducing the same topology on N will have identical charts and will consequently coincide. □

Of course, by varying the topology we may obtain different submanifold structures on N. For example, any submanifold $N \subset M$ can be provided with a discrete topology, thus turning it into a zero-dimensional submanifold.

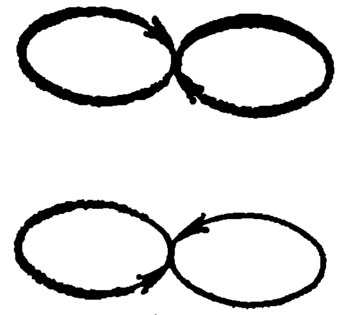
A less trivial example is obtained if we consider in $\mathbb{R}^2$ an open square $-1 < x < 1$, $-1 < y < 1$. In the induced topology it is a two-dimensional open submanifold. It can be turned, however, into a one-dimensional submanifold if we introduce a topology whose open sets are the sets intersecting with every vertical interval $x = x_0$, $-1 < y < 1$ the intersections being an open set (in that interval). The resulting submanifold consists of an uncountable number of components, each being diffeomorphic to the straight line

$\mathbb{R}$. We shall call it a *dissected square*.

Such pathologic possibilities will be excluded if we impose on submanifolds the condition that there should be a *countable base*.



A



B

There are, however, other possibilities of varying topology. Consider, for example, in the plane $\mathbb{R}^2$ the figure of eight set represented in Fig. A. In the topology induced by the topology of the plane, this subset is not a submanifold. But it can be turned into a submanifold, there being even two methods of doing so, if we introduce the stronger topologies represented schematically in Fig. B. In both cases the resulting submanifold is diffeomorphic to the straight line $\mathbb{R}$ and is therefore connected and has a countable base unlike the previous manifolds.

Definition 6. An (m-dimensional) submanifold N of an (n-dimensional) manifold M is said to be *locally rectifiable* at a point $a \in N$ if there is a chart (U, h) of M and a subset $\Xi \subset \mathbb{R}^{n-m}$ such that $a \in U$ and in the topology induced by the topology of N the intersection $U \cap N$ is the union of flat (see p. 210) submanifolds V_ξ, $\xi \in \Xi$, of the chart (U, h):

$$U \cap N = \bigcup_{\xi \in \Xi} V_\xi.$$

A submanifold N is said to be *locally rectifiable* if it is locally rectifiable at each of its points.

The submanifolds of Fig. B are not locally rectifiable.

The "parametrizing" set Ξ may in general be arbitrary and the fact that it exists is not enough by itself to guarantee against pathologies. For example, a dissected square is locally rectifiable, and for any of its points the set Ξ is an interval. In less pathologic situations, however, this set cannot be too large. For example, it is immediate from the fact that all submanifolds V_ξ are obviously open in N

that *if a locally rectifiable submanifold N has a countable base, then for any point a of N the set Ξ is at most countable.*

It is also worth while keeping in mind that as it follows immediately from the definition of an induced topology, *if the topology of a submanifold N is induced by the topology of a universal manifold M, then the manifold N is locally rectifiable and for any of its points the set Ξ can be chosen to consist of a single point.*

Thus locally rectifiable submanifolds can be considered as generalizations of submanifolds with induced topology.

To avoid constant reservations we shall henceforth once and forever assume that all the charts (U, h) under consideration are *cubic*, i.e. that the set $h(U) \subset \mathbb{R}^n$ is a cube

$$|x^1| < c, \ldots, |x^n| < c.$$

The number c will be called the *half-width of a chart* (U, h).

Then for $|\xi^1| < c, \ldots, |\xi^{n-m}| < c$ every flat submanifold V_ξ is connected (and nonempty).

Therefore, in particular, for a submanifold N locally rectifiable at a point a, all flat manifolds V_ξ, $\xi \in \Xi$ constituting an intersection $U \cap N$ are components of connectedness of that intersection in the topology induced by the topology of N. The example of a dissected square shows that as regards the topology of the containing manifold M this is in general false. If, however, the *submanifold N has a countable base, then submanifolds V_ξ are components of $U \cap N$ in the topology induced by the topology of M as well.* Indeed, the mapping $U \cap N \to \Xi$ defined by the formula

$$a \mapsto (x^{m+1}(a), \ldots, x^n(a)) \tag{2}$$

is obviously continuous (in the topology of M). It therefore sends every component of the set $U \cap N$ to a component of Ξ. But since Ξ is countable, as was noticed above, its components are points. Therefore every component of the set $U \cap N$ is contained in the inverse image V_ξ of some point $\xi \in \Xi$ under mapping (2) and hence coincides with V_ξ. $\square$

Lemma 2. *Let P and M be smooth manifolds and N be a locally rectifiable submanifold of M having a countable base. Also let $\iota\colon N \to M$ be an embedding and $\Phi\colon P \to N$ be a map-*

ping of P into N such that the composition $\iota \circ \Phi$: $P \to M$ is a continuous mapping. Then Φ is also continuous.

If in addition the mapping $\iota \circ \Phi$ is smooth, then Φ is also smooth.

$$\begin{tikzcd} & N \arrow[d, "\iota"] \\ P \arrow[ur, "\Phi"] \arrow[r, "\iota\circ\Phi"'] & M \end{tikzcd}$$

Proof. Let $b \in P$ and $a = \Phi(b)$.

By definition there is a cubic chart (U, h) (for which $h(a) = 0$) in M, such that the intersection $U \cap N$ in the induced topology is the union of a countable number of connected flat submanifolds V_ξ, $\xi \in \Xi$. Since the mapping $\iota \circ \Phi$ is continuous, there is in P a neighbourhood W of a point b whose image $(\iota \circ \Phi)(W)$ is contained in U and hence in $U \cap N$. It may be assumed without loss of generality that W is connected. Then (under a continuous mapping a connected set goes over into a connected set) the image $(\iota \circ \Phi)(W)$ of W under the mapping $\iota \circ \Phi$ is also connected and is hence contained in one of the components V_ξ of the set $U \cap N$. Since $\Phi(b) = a$ and $a \in V_0$, that component is necessarily $V_0 = V$. Thus for the neighbourhood V of a in the manifold N there is a neighbourhood W of b in P such that $\Phi(W) \subset V$. Since neighbourhoods of the form V constitute the fundamental system (base) of neighbourhoods of a in N, this proves that the mapping Φ: $P \to N$ is continuous at b. Since $b \in P$ is an arbitrary point, the mapping Φ is consequently continuous.

Now let $\iota \circ \Phi$ be a smooth mapping. To prove that Φ is a smooth mapping, one must prove that for any function g smooth in N the function $g \circ \Phi$ is smooth in P. But by Lemma 1 g is locally of the form $f \circ \iota$, where f is some function smooth in M. The function $g \circ \Phi$ therefore locally coincides with the smooth function $f \circ (\iota \circ \Phi)$ and is therefore smooth. $\square$

The example of manifolds in Fig. B shows that without the condition of local rectifiability Lemma 2 is false.

Now we are in a position to prove the uniqueness theorem at which we aimed.

Proposition 3. *If it is possible to introduce into a submanifold N the structure of a locally rectifiable submanifold with a countable base, then this can be done only in a unique way.*

Proof. Let N' and N'' be locally rectifiable submanifolds with a countable base with N being a set of points for the submanifolds. Then it will be possible to apply Lemma 2 to the identity mapping $N' \to N''$. That mapping therefore will be smooth. By the same reasoning so will the identity mapping $N'' \to N'$. Hence the smoothnesses on N' and N'' coincide. □

Corollary. *Let N be a locally rectifiable submanifold with a countable base of a smooth manifold M and let Φ: $M \to M$ be a diffeomorphism of M onto itself such that $\Phi a \in N$ and $\Phi^{-1}a \in N$ for any point $a \in N$. Then the mapping $N \to N$ induced by Φ is also a diffeomorphism.*

Proof. Let N' be the image of N under Φ. Obviously N' is also a locally rectifiable submanifold with a countable base. In addition, under the hypothesis N' being a set coincides with N. By Proposition 2, therefore N' being a manifold coincides with N as well. Hence the diffeomorphism $N \to N'$ induced by Φ will in fact be a diffeomorphism $N \to N$. □

In connection with the results obtained the question arises as to the conditions ensuring that a submanifold has a countable base. We show that for a connected submanifold to have a countable base it is sufficient that the containing manifold M have a countable base.

Lemma 3. *Suppose for a connected topological space X, there is an open covering $\{U_\alpha\}$ such that*

(i) *every set U_α (provided with the topology of a subspace) is a space with a countable base;*

(ii) *for any α_0 there is at most a countable number of sets U_α intersecting with U_{α_0}.*

Then X has a countable base.

Proof. It suffices to show that X is the union of a countable (or finite) subfamily of $\{U_\alpha\}$. On fixing some $U_{\alpha_0} \neq \varnothing$ consider all possible elements U_α of a given covering for which there is a finite sequence

$$U_{\alpha_1}, U_{\alpha_2}, \ldots, U_{\alpha_n}$$

of the elements of $\{U_\alpha\}$, such that $U_{\alpha_n} = U_\alpha$ and $U_{\alpha_{i-1}} \cap U_{\alpha_i} \neq \varnothing$ for any $i = 1, \ldots, n$. It is immediate from condition (ii) that all such elements constitute at most a countable subfamily of $\{U_\alpha\}$. Let X' be their union. Clearly X' is open (and nonempty). But it is also closed, for if $x \in \overline{X}'$ and $x \in U_\alpha$, then $X' \cap U_\alpha \neq \varnothing$ and therefore U_α intersects with some element of the subfamily constructed and hence is itself in that subfamily. Therefore $U_\alpha \subset X$ and hence $x \in X$. The set X', being an open and closed nonempty subset of the connected space X, must coincide with the entire X. Consequently, X has a countable base. □

Lemma 4. *Suppose that for a connected space X there is an open countable covering $\{U_k\}$ each element U_k of which is the union of disjoint open sets U_{k,α_n} having a countable base. Then X is also a space with a countable base.*

Proof. It suffices to show that the open covering $\{U_{k,\alpha_k}\}$ satisfies condition (ii) of Lemma 3. Since $\{U_k\}$ is countable, it suffices to show that for any k, l and α_k, there is at most a countable number of sets U_{l,α_l} intersecting with U_{k,α_k}. Suppose this is not the case, i.e. let there be an uncountable family of sets U_{l,α_l} intersecting with U_{k,α_k}. By choosing in each intersection a point we obtain in U_{k,α_k} an uncountable subset consisting of isolated points (recall that U_{l,α_l} are disjoint sets under the hypothesis). Since any discrete subset of a space with a countable base is at most countable, the existence of such an uncountable subset contradicts the fact that U_{k,α_k} is a space with a countable base. Hence at most a countable number of sets U_{l,α_l} intersect with U_{k,α_k}. □

Corollary 1. *Any space covering a space with a countable base also has a countable base.*

Proof. The inverse images of the elements of a countable covering which consists of evenly covered sets constitute a covering of a covering space, that satisfies the conditions of Lemma 4. □

Corollary 2. *If there is a locally homeomorphic mapping*

$$f\colon X \to \mathbb{R}^m$$

for a connected space X then X has a countable base.

Proof. Let $\{U_k\}$ be a countable base of a space $\mathbb{R}^m$, the

former consisting of connected open sets (of parallelepipeds, for example), and let $V_{k,\alpha}$ be open subsets of X homeomorphically mapped by f onto U_k (here α ranges over some set of indices A that depends on k and that can be empty for some k). The local homeomorphism of f implies that the sets

$$V_k = \bigcup_{\alpha \in A_k} V_{k,\alpha}$$

cover the entire X. Consequently, to apply Lemma 4, it is necessary only to show that the connected open sets $V_{k,\alpha}$ are components of the sets V_k, i.e. that for any α, $\beta \in A_k$, $V_{k,\alpha} = V_{k,\beta}$, if $V_{k,\alpha} \cap V_{k,\beta} \neq \varnothing$.

Let $W = V_{k,\alpha} \cap V_{k,\beta} \neq \varnothing$ and let

$$g_\alpha \colon U_k \to V_{k,\alpha}, \qquad g_\beta \colon U_k \to V_{k,\beta}$$

be the homeomorphisms inverse to homeomorphisms $f|_{V_{k,\alpha}}$ and $f|_{V_{k,\beta}}$. If $x_n \in W$ and $x = \lim x_n$, then $f(x) = \lim f(x_n)$ and $g_\beta(f(x_n)) = x_n$. Therefore

$$g_\beta(f(x)) = \lim g_\beta(f(x_n)) = \lim x_n = x.$$

Consequently, if $x \in V_{k,\alpha}$ (and therefore $f(x) \in U_k$), then $x \in V_{k,\beta}$, i.e. $x \in W$. This shows that W is closed in $V_{k,\alpha}$. Since W is also open in $V_{k,\alpha}$ (and nonempty) and $V_{k,\alpha}$ is connected (as it is homeomorphic to the connected set U_k), this is possible only when $V_{k,\alpha} = W$. In a similar manner it can be proved that $V_{k,\beta} = W$. Consequently $V_{k,\alpha} = V_{k,\beta}$. $\square$

Corollary 3. *Any connected submanifold N of a manifold $\mathbb{R}^n$ has a countable base.*

Proof. Let $x^1, \ldots, x^n$ be coordinates in $\mathbb{R}^n$ (relative to some basis) and let $\iota \colon N \to \mathbb{R}^n$ be an embedding. Consider a collection $\alpha = (i_1, \ldots, i_m)$ of indices $1, \ldots, n$ (with m being the dimension of the manifold N) and a subset V_α of N. V_α consists of points $a \in N$ in the neighbourhood of each of which the functions $x^{i_1} \circ \iota, \ldots, x^{i_m} \circ \iota$ are local coordinates. It is clear that V_α is open in N. In addition (see Proposition 3) any point $a \in N$ is at least in one of the sets V_α. Let V'_α be a component of a set V_α. By construction, the mapping $V'_\alpha \to \mathbb{R}^m$ defined by the formula

$$a \mapsto (x^{i_1}(a), \ldots, x^{i_m}(a)), \quad a \in V'_\alpha$$

is a local homeomorphism. Hence by Corollary 2 the connected set V'_α has a countable base. Thus a finite open cov-

ering $\{V_\alpha\}$ of N satisfies the conditions of Lemma 4. Therefore N has a countable base. □

Now we are ready to prove the statement announced above:

Proposition 4. *Any connected submanifold N of a manifold M with a countable base is itself a manifold with a countable base.*

Proof. Let $\{U_k\}$ be a countable covering of M, the former consisting of coordinate neighbourhoods and let $V_k = U_k \cap N$. The sets V_k are open in N and any point $a \in N$ is at least in one of them. Every component V_k' of a set V_k is a connected smooth manifold diffeomorphic to some submanifold of $\mathbb{R}^m$. Therefore by Corollary 3 that component has a countable base. This means that the open covering $\{V_k\}$ of the manifold N satisfies all the conditions of Lemma 4. Therefore N has a countable base. □

The applicability of the above results to Lie groups is ensured by the following proposition:

Proposition 5. *Any connected Lie group G has a countable base.*

Proof. Let U be a neighbourhood of the identity of a group diffeomorphic to an open set of a space $\mathbb{R}^n$ and having the property that $U^{-1} = U$. On choosing in U a countable everywhere dense set Y consider the set Z of all elements of G of the form $y_1y_2 \ldots y_k$, where $y_1, \ldots, y_k \in Y$ (with k arbitrary). Clearly Z is countable. Since G is connected, it is generated by U, i.e. any element x of G is of the form $x_1x_2 \ldots x_k$, where $x_1, x_2, \ldots, x_k \in U$. Let $x_{(i)} = x_1x_2 \ldots x_i$, $i = 1, \ldots, k$ (in particular $x_{(1)} = x_1$ and $x_{(k)} = x$). It can be derived immediately from the continuity of multiplication in G by an obvious induction that the identity of G has a neighbourhood V such that

$$V \cdot x_{(1)} V x_{(1)}^{-1} \cdot x_{(2)} V x_{(2)}^{-1} \cdot \ldots \cdot x_{(k)} V x_{(k)}^{-1} \subset U.$$

Since Y is everywhere dense in U, there is a point $y_i \in Y$ in the neighbourhood Vx_i of a point $x_i \in U$. Let $v_i = y_i x_i^{-1} \in V$. Then

$$\begin{aligned} y_1y_2 \ldots y_k &= v_1x_1 \cdot v_2x_2 \cdot \ldots \cdot v_kx_k \\ &= v_1 \cdot x_{(1)}v_2x_{(1)}^{-1} \cdot x_{(1)}v_3x_{(2)}^{-1} \cdot \ldots \cdot x_{(k-1)}v_kx_{(k)}^{-1} \cdot x_{(k)} = ux, \end{aligned}$$

where $u \in U$. This shows that the point $z = y_1 \ldots y_k \in Z$ has the property that $x \in Uz$ (recall that under the hypothesis $U^{-1} = U$). This proves that open sets of the form Uz, $z \in Z$, cover G. Since Z is countable and sets Uz (homeomorphic to the set U) have a countable base, it follows immediately that G has also a countable base. □

Corollary. *Any connected submanifold of a connected Lie group is a manifold with a countable base.*

In particular, the maximal integral manifold H of the subfibering $E^{\mathfrak{h}}$ we are concerned with in the first place is a submanifold with a countable base. It is easily seen that it is locally rectifiable. Indeed, *in any manifold M every maximal integral manifold W of an integrable subfibering E is locally rectifiable.* Indeed, as we know, M can be covered by charts having the property that each of their flat submanifolds V_{ξ} is an integral manifold of the subfibering E. Therefore the intersection of W with every such chart is the union of some of these submanifolds, by virtue of the maximality of W which means by definition that the manifold W is locally rectifiable. □

Remark 2. That the integral manifold H is locally rectifiable follows also from the general lemma below.

Lemma 5. *A connected submanifold H of a Lie group G, for which the set H_{abstr} is a subgroup of the group G_{abstr}, is locally rectifiable.*

Proof. As we know, there is a chart $(U, x^1, \ldots, x^n)$ at the point e in G, such that the flat submanifold

$$V\colon\ x^{m+1} = 0, \ldots, x^n = 0$$

is a neighbourhood of e in H and a local subgroup of a local group U. In the Lie algebra such that $\mathfrak{l}(G) = \mathfrak{l}(U)$ subalgebra $\mathfrak{h} = \mathfrak{l}(V)$ corresponds to the subgroup.

Without loss of generality we may clearly assume the coordinates $x^1, \ldots, x^n$ to be canonical coordinates defined by some decomposition $\mathfrak{l}(G) = \mathfrak{h} \oplus \mathfrak{k}$. Then (see Lecture 7) the flat submanifolds V_{ξ} of the chart U will be cosets $aV = aH \cap U$ of the local subgroup V. Since the intersection $U \cap H$ is the union of cosets aV such that $a \in U \cap H$, this proves that the intersection $U \cap H$ is the union of some flat

submanifolds V_ξ. Hence the submanifold H is locally rectifiable at e.

Now let a be an element of H. Consider a diffeomorphism $L_a\colon G \to G$. This maps H onto itself and sends the point e to the point a. Hence H is locally rectifiable at a too. $\square$

Since H has a countable base and is locally rectifiable, by virtue of Lemma 2 *every mapping* $\Phi\colon P \to H$ *of a smooth manifold* P *into the integral manifold* H, *having the property that its composition*

$$\iota \circ \Phi\colon P \to G$$

with an embedding $\iota\colon H \to G$ *is smooth, is a smooth mapping.*

We apply that statement to the manifold $P = H \times H$ and to the mapping $\mu_H\colon (x, y) \mapsto xy$. Since we have the commutative diagram

$$\begin{tikzcd} H \times H \arrow[r, "\mu_H"] \arrow[d, "\iota \times \iota"'] & H \arrow[d, "\iota"] \\ G \times G \arrow[r, "\mu_G"'] & G \end{tikzcd}$$

and the mappings $\iota \times \iota$ and μ_G are smooth, the mapping $\iota \circ \mu_H$ is smooth. Hence so is the mapping μ_H.

This proves that the *maximal invariant manifold* H *of the subfibering* $E^{\mathfrak{h}}$ *is a Lie group and hence a subgroup of a Lie group* G.

We shall denote this subgroup by $G(\mathfrak{h})$.

Remark 3. By virtue of Lemma 5 the above reasoning also proves that a *connected submanifold* H *of a Lie group* G *is its subgroup if the set* H_{abstr} *is a subgroup of the group* G_{abstr}.

Since the subspace $E_e^{\mathfrak{h}} = \mathfrak{h}$ is the tangent space at e to the subgroup $H = G(\mathfrak{h})$ the *given subalgebra* $\mathfrak{h}$ *is the Lie algebra of* H.

Now we are ready to prove Theorem 1.

Proof of Theorem 1. We already know that any subgroup H of a Lie group G has the corresponding subalgebra $\mathfrak{h} =$

$\mathfrak{l}(H)$ of the Lie algebra $\mathfrak{g} = \mathfrak{l}(G)$ and any subalgebra $\mathfrak{h} \subset \mathfrak{g}$ has the corresponding connected subgroup $H = G(\mathfrak{h})$, with $\mathfrak{l}(H) = \mathfrak{h}$. To complete the proof of Theorem 1 therefore it remains only to show that for every connected subgroup H of G we have $H = G(\mathfrak{h})$, where $\mathfrak{h} = \mathfrak{l}(H)$. But the subgroups H and $G(\mathfrak{h})$ have the same Lie algebra $\mathfrak{h}$ and therefore if considered as local groups they coincide (see Lecture 7). This means that H and $G(\mathfrak{h})$ have the same neighbourhoods of the identity. Consequently $H = G(\mathfrak{h})$, since being connected the groups H and $G(\mathfrak{h})$ are generated by every neighbourhood of the identity. □

Lecture 12

Alternative definitions of a subgroup of a Lie group · Topological subgroups of Lie groups · Closed subgroups of Lie groups · Algebraic groups · Groups of automorphisms of algebras · Groups of automorphisms of Lie groups · Ideals and invariant subgroups · Quotient manifolds of Lie groups · Quotient groups of Lie groups · The calculation of fundamental groups · The simple-connectedness of groups SU(n) *and* Sp(n) · *The fundamental group of a group* U(n)

Remark 3 of Lecture 11 gives us an alternative definition of a subgroup of a Lie group that is formally broader. It turns out that the conditions imposed on subgroups of Lie groups can be relaxed in other directions as well.

A smooth mapping Φ: $N \to M$ is said to be an *immersion* if for any point $a \in N$ the linear mapping

$$(d\Phi)_a: \mathsf{T}_a(N) \to \mathsf{T}_{\Phi a}(M)$$

is a monomorphism (i.e. the mapping is injective).

Proposition 1. *Any monomorphism* Φ: $H \to G$ *of Lie groups is an immersion.*

Proof. Consider the exponent

$$\exp: \mathfrak{l}(G) \to G.$$

In the interpretation of the elements of $\mathfrak{l}(G)$ as one-parameter subgroups that mapping is defined by the formula

$$\exp \beta = \beta(1).$$

Since $\mathfrak{l}(\Phi)\beta = \Phi \circ \beta$ (Proposition of 5 Lecture 2), it follows that there is a commutative diagram

$$\begin{tikzcd} \mathfrak{l}(H) \arrow[r, "\mathfrak{l}(\Phi)"] \arrow[d, "\exp"'] & \mathfrak{l}(G) \arrow[d, "\exp"] \\ H \arrow[r, "\Phi"'] & G \end{tikzcd}$$

If the linear mapping $\mathfrak{l}(\Phi) = (d\Phi)_e$ is not injective, then in the normal neighbourhood of zero of the algebra $\mathfrak{l}(H) = \mathsf{T}_e(H)$ there is a nonzero vector A which is in the kernel of $\mathfrak{l}(\Phi)$, i.e. such that $\mathfrak{l}(\Phi)A = 0$. But then

$$(\Phi \circ \exp) A = (\exp \circ \mathfrak{l}(\Phi)) A = \exp 0 = e$$

and hence $\exp A = e$ (for Φ is injective). Since this is impossible (in a normal neighbourhood the mapping exp is a diffeomorphism), this proves that the mapping $(d\Phi)_e$ is monomorphic.

On the other hand, the fact that the mapping Φ is a homomorphism implies that for any element $a \in H$ we have

$$\Phi \circ L_a = L_{\Phi a} \circ \Phi.$$

For differentials this means that there is a commutative diagram

$$\begin{tikzcd} \mathbf{T}_e(H) \arrow[r, "(dL_a)_e"] \arrow[d, "(d\Phi)_e"'] & \mathbf{T}_a(H) \arrow[d, "(d\Phi)_a"] \\ \mathbf{T}_e(G) \arrow[r, "(dL_{\Phi a})_e"'] & \mathbf{T}_{\Phi a}(G) \end{tikzcd}$$

from which it follows (the horizontal arrows of the diagram being isomorphisms) that the mapping $(d\Phi)_a$ is also monomorphic. $\square$

Corollary. *A Lie group H for which H_{abstr} is a subset in G_{abstr} and an embedding $\iota\colon H \to G$ is a homomorphism of Lie groups is a subgroup of a Lie group G.*

Proof. By Proposition 1 the mapping ι is an immersion, and this precisely means that H is a subgroup of a Lie group G. $\square$

By virtue of this corollary the *matrix Lie groups introduced by Definition* 1 *of Lecture* 3 *are nothing but subgroups of the Lie group* GL $(n; \mathbb{R})$.

Of paramount interest, of course, are subgroups H of a Lie group G whose topology is induced by that of G, i.e. for which the topological group H_{top} is a subgroup of G_{top}. We shall call such subgroups *topological subgroups* of Lie groups.

Recall that a subset A of a topological space X is said to be *locally closed* if any point $a \in A$ has in X a neighbourhood U such that the intersection $A \cap U$ is closed in U. We have already met with the notion in Lecture 7 in connection with local subgroups. We shall need the following lemma from the theory of topological groups:

Lemma 1. *Any locally closed subgroup H of a topological group G is closed.*

Proof. Let U be a neighbourhood of a point e, such that $H \cap U$ is closed in U. Clearly, it may be assumed without loss of generality that $U^{-1} = U$. Consider a point $x \in \overline{H}$. Then $xU \cap H \neq \varnothing$. Let $y \in xU \cap H$. Since the left shift L_y: $a \mapsto ya$ is a homeomorphism, the set $y(U \cap H)$ is closed in yU. But since $y \in H$, we have $y(U \cap H) = yU \cap H$. Hence $yU \cap H$ is closed in yU, i.e. $\overline{yU \cap H} \cap yU = yU \cap H$. On the other hand, $x \in yU^{-1} = yU$ and therefore $x \in yU \cap \overline{H} \subset \overline{yU \cap H}$. Consequently $x \in yU \cap H$ and hence $x \in H$. $\square$

A subgroup H of a Lie group G will be said to be *closed* if the set of its points is a closed subset in G.

Note that the topology of the subgroup H itself does not figure at all in this definition. Nevertheless it turns out that the closure condition uniquely fixes that topology:

Proposition 2. *A subgroup H of a Lie group G is closed if and only if its topology is induced by that of G, i.e. if it is a topological subgroup.*

Proof. By virtue of Lemma 1, we prove the sufficiency of that condition if we establish that *every submanifold N whose topology is induced by the topology of the containing*

manifold M, is locally closed. This is nearly obvious. Indeed, any point of such a submanifold has in M a neighbourhood U that intersects with N in some flat submanifold V in U. On the other hand, it is clear that any flat submanifold is locally closed.

To prove necessity we use the fact that every closed subgroup H of a Lie group G is a locally rectifiable submanifold with a countable base. Therefore there is a neighbourhood U of the identity e in G, such that the intersection $U \cap H$ is the union of a countable number of flat submanifolds V_ξ, $\xi \in \Xi \subset \mathbb{R}^{n-m}$. Since H is a closed subgroup, the set (which is the image of the set $U \cap H$ under the continuous mapping defined by formula (2) of Lecture 11) is locally closed. Consequently, being countable, it has at least one isolated point ξ_0. The corresponding flat submanifold V_{ξ_0} has the property that any point a of it has in U a neighbourhood U_a such that the intersection $U_a \cap H$ is in V_{ξ_0} and is hence a neighbourhood of a in H. This means that a has in U (and hence in G) a fundamental system of neighbourhoods that cuts on H a fundamental system of neighbourhoods of a in H. By applying a left shift $L_{ba^{-1}}$ we find that this property holds for any point $b \in H$ as well. Then by definition, the topology in H will just be induced by the topology of the containing space G. □

By virtue of the corollary of Lemma 1 in Lecture 11 (or if you please by virtue of Proposition 3 of Lecture 4) it follows from Proposition 1 that *on every closed subgroup H of a Lie group G its smooth-manifold structure is unique.*

It is surprising that the closure condition by itself should be quite enough for H to have a smoothness with respect to which it is a Lie group and a subgroup of the Lie group G:

Theorem 1 (Cartan). *If a closed subset H of a Lie group G is a subgroup of G_{abstr}, then H has a unique smoothness (compatible with the topology induced on H) with respect to which H is a subgroup of the Lie group G (and, in particular, a Lie group).*

Proof. Every Lie group G is at the same time a local Lie group. Since H is closed, for any neighbourhood U of e in the local group G the intersection $U \cap H$ is closed in U. Hence H is a local subgroup of a local Lie group G (see Definition 1 of Lecture 7). Therefore by the Cartan theorem for local groups (Proposition 1 of Lecture 7) the local

group H is locally flat, i.e. in other words, its intersection $U \cap H$ with some chart U at e is a flat submanifold of U of the form $\exp \mathfrak{h}$, where $\mathfrak{h}$ is some subalgebra of a Lie algebra $\mathfrak{g} = \mathfrak{l}(G)$. This means that H locally coincides at e with a connected subgroup $G(\mathfrak{h})$ of a Lie group G. Since any neighbourhood of a connected topological group generates the entire group (Lemma 3 of Lecture 9), this proves that the group $G(\mathfrak{h})$ (more precisely, the group $G(\mathfrak{h})_{\text{abstr}}$ provided with an induced topology) coincides with the component of the identity H_e of the group H. This introduces into the group H_e and hence into the entire group H a smoothness with respect to which that group is a subgroup of the Lie group G.

The uniqueness of that smoothness is ensured, according to the remark above, by the closure of the subgroup H. □

Notice that by virtue of being closed the subgroup H of the Lie group G is its topological subgroup.

Theorem 1 is the most powerful tool for establishing whether or not a particular topological group is a Lie group.

Example. A subgroup of $\mathrm{GL}(n, \mathbb{R})$ (or of $\mathrm{GL}(n; \mathbb{C})$) is said to be an *algebraic group* if it is an intersection of $\mathrm{GL}(n; \mathbb{R})$ (or $\mathrm{GL}(n; \mathbb{C})$) with an *algebraic variety in a space* $\mathbb{R}(n) = \mathbb{R}^{n^2}$ (or in $\mathbb{C}(n) = \mathbb{C}^{n^2}$ respectively), i.e. with the set of general zeros of some system of polynomials in n^2 unknowns.

Since any algebraic variety is clearly closed, we find by Theorem 1 that *every algebraic group is a matrix Lie group.*

This immediately proves that the groups considered in Lecture 1 ($\mathrm{SL}(n)$, $\mathrm{O}(n)$, $\mathrm{Sp}(n)$, $\mathrm{U}(n)$, etc.) are all Lie groups (notice that $\mathrm{U}(n)$ should be treated not as a subgroup of $\mathrm{GL}(n; \mathbb{C})$ but, by virtue of the embedding $\mathrm{GL}(n; \mathbb{C}) \subset \mathrm{GL}(2n; \mathbb{R})$, as a subgroup of $\mathrm{GL}(2n; \mathbb{R})$).

Let $\mathcal{A}$ be a finite-dimensional algebra over a field $\mathbb{R}$ or $\mathbb{C}$ (in general neither an associative nor Lie one) and let $e_1, \ldots, e_n$ be its basis. Clearly, an invertible linear mapping $\Phi: \mathcal{A} \to \mathcal{A}$ is an automorphism of $\mathcal{A}$ if and only if $\Phi(e_i e_j) = \Phi(e_i)\Phi(e_j)$ for any $i, j = 1, \ldots, n$. Consequently if $\Phi(e_i) = x_i^j e_j$ and $e_i e_j = c_{ij}^k e_k$ and hence

$$\Phi(e_i e_j) = \Phi(c_{ij}^k e_k) = c_{ij}^k x_k^l e_l,$$
$$\Phi(e_i)\Phi(e_j) = (x_i^p e_p)(x_j^q e_q) = c_{pq}^l x_i^p x_j^q e_l,$$

then Φ is an automorphism if and only if

$$c_{ij}^{k} x_k^l = c_{pq}^{l} x_i^p x_j^q$$

for any i, j, $l = 1, \ldots, n$. This means that the matrices (x_i^j) corresponding to the automorphisms of $\mathcal{A}$ constitute an algebraic, and hence smooth, group. Thus giving a basis $e_1, \ldots, e_n$ defines an isomorphism of a group of automorphisms Aut $\mathcal{A}$ of $\mathcal{A}$ onto some matrix algebraic Lie group. The Lie-group structure transferred to Aut $\mathcal{A}$ with the aid of that isomorphism is clearly independent of the choice of basis $e_1, \ldots, e_n$. Thus the *group* Aut $\mathcal{A}$ *of automorphisms of a finite-dimensional algebra* $\mathcal{A}$ *is a Lie group.*

Let us find the Lie algebra of that group.

Proposition 2. *The Lie algebra* Der $\mathcal{A}$ *of all differentiations of an algebra* $\mathcal{A}$ *is the Lie algebra of* Aut $\mathcal{A}$:

$$\mathfrak{l}(\mathrm{Aut}\,\mathcal{A}) = \mathrm{Der}\,\mathcal{A}.$$

Proof. On choosing in $\mathcal{A}$ a basis we may assume that Aut $\mathcal{A}$ and Der $\mathcal{A}$ consist of matrices.

Let $D \in$ Der $\mathcal{A}$. Then for any elements $x, y \in \mathcal{A}$ and any $p \geqslant 0$

$$D^p(xy) = \sum_{i=0}^{p} \binom{p}{i} D^i x \cdot D^{p-i} y \quad (\textit{the Leibnitz formula})$$

and hence

$$\begin{aligned}(e^{tD})(xy) &= \sum_{p=0}^{\infty} \frac{t^p}{p!} D^p(xy) \\ &= \sum_{p=0}^{\infty} \sum_{i=0}^{p} \frac{1}{p!} \binom{p}{i} t^p \cdot D^i x \cdot D^{p-i} y \\ &= \sum_{i=0}^{\infty} \sum_{j=0}^{\infty} \frac{t^{i+j}}{i!\,j!} D^i x \cdot D^j y \\ &= \left(\sum_{i=0}^{\infty} \frac{t^i}{i!} D^i x\right) \left(\sum_{j=0}^{\infty} \frac{t^j}{j!} D^j x\right) = e^{tD}x \cdot e^{tD} y\end{aligned}$$

(the convergence of all series is ensured by standard calculations using matrix norms). This means that $e^{tD} \in$ Aut $\mathcal{A}$

and hence that $D \in \mathfrak{l}(\operatorname{Aut} \mathcal{A})$.

Conversely, let $D \in \mathfrak{l}(\operatorname{Aut} \mathcal{A})$, i.e. $e^{tD} \in \operatorname{Aut} \mathcal{A}$. Then

$$\begin{aligned}(e^{tD} - E)(xy) &= e^{tD}x \cdot e^{tD}y - x \cdot y \\ &= (e^{tD}x - x)\, e^{tD}y + x\,(e^{tD}y - y)\end{aligned}$$

and hence

$$\begin{aligned} D(xy) &= \lim_{t \to 0} \frac{(e^{tD} - E)(xy)}{t} = \lim_{t \to 0} \frac{e^{tD}x - x}{t} e^{tD}y + \lim_{t \to 0} x \frac{e^{tD}y - y}{t} \\ &= Dx \cdot y + x \cdot Dy. \end{aligned}$$

Consequently $D \in \operatorname{Der} \mathcal{A}$. $\square$

Suppose, in particular, that $\mathcal{A}$ is the Lie algebra $\mathfrak{g}$ of a simply connected Lie group G. Since the Lie functor is completely univalent on the category of simply connected Lie groups (see Lecture 10), any automorphism $\mathfrak{g} \to \mathfrak{g}$ of the Lie algebra $\mathfrak{g}$ is realized by some automorphism $G \to G$ of G. This shows that the *group of automorphisms* $\operatorname{Aut} G$ *of the simply connected Lie group G is isomorphic to the group of automorphisms* $\operatorname{Aut} \mathfrak{g}$ *of its Lie algebra* $\mathfrak{g}$:

$$\operatorname{Aut} G \approx \operatorname{Aut} \mathfrak{g}.$$

By transferring by means of this isomorphism the smoothness from $\operatorname{Aut} \mathfrak{g}$ into $\operatorname{Aut} G$ we define $\operatorname{Aut} G$ as a Lie group. By virtue of the foregoing the *Lie algebra* $\operatorname{Der} \mathfrak{g}$ *will be the Lie algebra of the Lie group* $\operatorname{Aut} G$:

$$\mathfrak{l}(\operatorname{Aut} G) = \operatorname{Der} \mathfrak{l}(G).$$

To obtain a similar result for a connected Lie group G, consider its universal covering group $\tilde{G}$. We know (see Lecture 9) that $\tilde{G}$ is functorially dependent on G and therefore any automorphism $\Phi\colon G \to G$ defines uniquely some automorphism $\tilde{\Phi}\colon \tilde{G} \to \tilde{G}$ for which there is a commutative diagram

$$\begin{tikzcd} \tilde{G} \arrow[r, "\tilde{\Phi}"] \arrow[d, "\pi"'] & \tilde{G} \arrow[d, "\pi"] \\ G \arrow[r, "\Phi"'] & G \end{tikzcd}$$

This defines a mapping (obviously a monomorphic one)

$$\operatorname{Aut} G \to \operatorname{Aut} \tilde{G}.$$

The image of that monomorphism consists of automorphisms $\Psi: \tilde{G} \to \tilde{G}$ for which $\pi(a) = \pi(b)$ yields $\pi\Psi(a) = \pi\Psi(b)$. This condition is precisely equivalent to the requirement that Ψ should send to itself the kernel $K = \operatorname{Ker} \pi$ of the covering π. Therefore the set of all such automorphisms is closed and is consequently (Theorem 1) a subgroup of the Lie group $\operatorname{Aut} \tilde{G}$ and hence a Lie group. By transferring this Lie-group structure into the group $\operatorname{Aut} G$ we define the latter group as a Lie group.

This proves that a *group of automorphisms of a connected Lie group is a Lie group.*

Let us now return to general Lie groups and their closed subgroups. Since a simply connected Lie group G can be reconstructed from its Lie algebra $\mathfrak{g} = \mathfrak{l}(G)$ in a unique way, all subalgebras $\mathfrak{h}$ of $\mathfrak{g}$ are correctly distributed in two classes: subgroups of the simply connected Lie group G correspond to subalgebras of one class and nonclosed ones to subalgebras of the other. The question thus arises as to the internal algebraic characterization of subalgebras of these classes or, equivalently, that of the corresponding subgroups. We shall not deal with this question in full generality and restrict our discussion to the following, perhaps most interesting and unexpected, result:

Theorem 2. *Any connected invariant subgroup H of a simply connected Lie group G is closed.*

We first prove a proposition characterizing Lie subalgebras which correspond to invariant subgroups:

Proposition 3. *The Lie algebra $\mathfrak{l}(H)$ of every invariant subgroup H of a Lie group G is an ideal of the Lie algebra $\mathfrak{l}(G)$ of the group G. Conversely, if a subgroup H is connected and the Lie algebra $\mathfrak{l}(H)$ is an ideal of the Lie algebra $\mathfrak{l}(G)$, then H is invariant.*

Proof. This proposition is quite similar to Proposition 2 of Lecture 7 and can be proved exactly in the same way. To avoid repeating ourselves, however, we shall give another proof here, one that relies on Proposition 2 of Lecture 7.

Clearly, by virtue of that proposition it suffices to prove

that a *connected Lie group H of a Lie group G is invariant if and only if a neighbourhood V of its identity is an invariant local subgroup of G* (considered as a local group). But, indeed, if H is invariant, then V is invariant by definition. Conversely, let V be invariant and let $g \in G$. Then there is a neighbourhood W of the identity such that $g^{-1}Wg \subset V$. Since the group H is connected, any element a of it is of the form $a_1a_2 \ldots a_k$, where $a_1, a_2, \ldots, a_k \in W$. Hence

$$g^{-1}ag = g^{-1}a_1g \cdot g^{-1}a_2g \cdot \ldots \cdot g^{-1}a_kg \in V \cdot V \cdot \ldots \cdot V \subset H$$

and therefore the subgroup H is invariant. $\square$

Notice that there are disconnected noninvariant subgroups H for which a subalgebra $\mathfrak{l}(H)$ is an ideal of the Lie algebra $\mathfrak{l}(G)$. Their components of the identity are invariant.

A substantial addition to Proposition 3 is the following proposition.

Proposition 4. *For any homomorphism $\Phi: G \to H$ of Lie groups its kernel* Ker Φ *is a subgroup of a Lie group G. The Lie algebra* $\mathfrak{l}$ (Ker Φ) *coincides with the kernel* Ker $\mathfrak{l}(\Phi)$ *of the induced mapping $\mathfrak{l}(\Phi): \mathfrak{l}(G) \to \mathfrak{l}(H)$ of Lie algebras*:

$$\mathfrak{l}(\operatorname{Ker} \Phi) = \operatorname{Ker} \mathfrak{l}(\Phi).$$

Proof. Since Ker Φ is closed, the first statement follows from Theorem 1. Every one-parameter subgroup $\beta: \mathbb{R} \to$ Ker Φ is sent by Φ to a constant mapping, i.e. to the zero of the algebra $\mathfrak{l}(H)$. Hence $\mathfrak{l}(\operatorname{Ker} \Phi) \subset \operatorname{Ker} \mathfrak{l}(\Phi)$. Conversely, if a one-parameter subgroup $\beta: \mathbb{R} \to G$ of G is in the kernel of $\mathfrak{l}(\Phi)$, then $\Phi \circ \beta = \text{const}$, i.e. $\beta(t) \in \operatorname{Ker} \Phi$ for all $t \in \mathbb{R}$ and hence $\beta \in \mathfrak{l}(\operatorname{Ker} \Phi)$. Consequently $\operatorname{Ker} \mathfrak{l}(\Phi) \subset \mathfrak{l}(\operatorname{Ker} \Phi)$.

Now we are in a position to prove Theorem 2.

Proof of Theorem 2. Let $\mathfrak{g} = \mathfrak{l}(G)$ and $\mathfrak{h} = \mathfrak{l}(H)$. Since H is invariant, the subalgebra $\mathfrak{h}$ is an ideal and therefore a quotient algebra $\mathfrak{g}/\mathfrak{h}$ is defined. By Theorem 1 of Lecture 10 (notice that so far the theorem has been proved by us only modulo the Ado theorem) there is a simply connected Lie group N with a Lie algebra $\mathfrak{g}/\mathfrak{h}$. Since on the category of simply connected Lie groups the Lie functor is completely univalent there is a homomorphism $\Phi: G \to N$ of Lie groups

that realizes a natural homomorphism φ: $\mathfrak{g} — \mathfrak{g}/\mathfrak{h}$, i.e. such that $\mathfrak{l}(\Phi) = \varphi$. By Proposition 4 the kernel Ker Φ of that homomorphism is a closed subgroup with a Lie algebra

$$\mathfrak{l}(\operatorname{Ker}\Phi) = \operatorname{Ker}\mathfrak{l}(\Phi) = \operatorname{Ker}\varphi = \mathfrak{h}.$$

The component of the identity $(\operatorname{Ker}\Phi)_e$ of that kernel is also closed and its Lie algebra is also the ideal $\mathfrak{h}$. Thus we have in G two connected subgroups H and $(\operatorname{Ker}\Phi)_e$ with the same Lie algebra. Therefore by Theorem 1 of the preceding lecture $H = (\operatorname{Ker}\Phi)_e$. Hence H is closed. □

Remark 1. Proposition 3 says that a Lie correspondence puts connected invariant subgroups of a Lie group into one-to-one correspondence with ideals of a Lie algebra $\mathfrak{g}$. Clearly, *if the group G is a direct product $A \times B$ of invariant subgroups A and B, then the Lie algebra $\mathfrak{g}$ will be a direct sum $\mathfrak{a} \oplus \mathfrak{b}$ of ideals $\mathfrak{a} = \mathfrak{l}(A)$ and $\mathfrak{b} = \mathfrak{l}(B)$*. The converse, however, is in general *false* even for connected lie groups G. If $\mathfrak{g} = \mathfrak{a} \oplus \mathfrak{b}$ and A, B are invariant subgroups of a connected group G, such that $\mathfrak{l}(A) = \mathfrak{a}$ and $\mathfrak{l}(B) = \mathfrak{b}$, then G is not necessarily a direct product $A \times B$ of the groups A and B. We can only say that G is generated by A and B (since any element of some normal neighbourhood is obviously a product of the elements of A and B, and G, being connected, is generated by that neighbourhood) and that the intersection $A \cap B$, being a subgroup of the Lie group G with a zero Lie algebra, is a zero-dimensional invariant subgroup. In particular, if $A \cap B$ is closed (which by virtue of Theorem 2 always holds if G is simply connected), then it is discrete. In addition, if the subgroups A and B are connected, then since it is continuous the mapping $(a, b) \mapsto aba^{-1}b^{-1}$ of a connected manifold $A \times B$ into a discrete manifold $A \cap B$ sends the entire manifold $A \times B$ to a point $e \in G$, i.e. A and B are commutative subgroups. Hence the mapping $A \times B \to G$ defined by the formula $(a, b) \mapsto ab$ is an epimorphism. Since the latter induces an identity isomorphism $\mathfrak{a} \oplus \mathfrak{b} \to \mathfrak{g}$ of Lie algebras, by Proposition 4 its kernel is discrete. The epimorphism thus is a group covering and therefore, for any simply connected group G, it is an isomorphism. This proves that a *simply connected Lie group G can be decomposed into a direct product $A \times B$ of connected subgroups A and B if*

and only if the Lie algebra $\mathfrak{g} = \mathfrak{l}(G)$ *can be decomposed into a direct sum* $\mathfrak{a} \dotplus \mathfrak{h}$ *of subalgebras* $\mathfrak{a} = \mathfrak{l}(A)$ *and* $\mathfrak{h} = \mathfrak{l}(B)$.

For any subgroup H of a Lie group G the components of left cosets aH, $a \in G$, are obviously nothing but all possible maximal invariant manifolds of a subfibering $E^{\mathfrak{h}}$, $\mathfrak{h} = \mathfrak{l}(H)$. There is therefore a (cubic) chart $(U, h) = (U, x^1, \ldots, x^n)$ in G, such that $e \in U$ and for any $a \in G$ the intersection $U \cap aH$ is a union of flat submanifolds of the form V_ξ, $\xi \in \mathbb{R}^{n-m}$. In particular, $U \cap H$ has this property. If H is closed (which is to be assumed throughout now), then the chart (U, h) can be chosen so that the intersection $U \cap H$ should consist of only one submanifold V_0 (see the proof of Proposition 1 above). Let W be a neighbourhood (cubic with respect to h) of the point e in G, such that $W^{-1} \subset W$ and $W^4 \subset U$. If the points $a, b \in W$ are congruent modulo H, i.e. $a^{-1}b \in H$, then $a^{-1}b \in W^2 \cap H \subset U \cap H = V_0$, i.e. $b \in aV_0$. Since $a \in aV_0$ and aV_0 together with V_0 is connected, this proves that a and b are in the same component of connectedness of $U \cap aH$, i.e. in the same manifold V_ξ. Since the converse is obvious (if $a, b \in W \cap V_\xi$, then $a^{-1}b \in H$), the points $a, b \in W$ are in the same coset mod H if and only if there is ξ such that $a, b \in V_\xi$, i.e. in other words, that the *intersections* $V_\xi \cap W$ *for different* ξ *are in different cosets mod* H.

We now consider the set G/H of all cosets aH, $a \in G$. The group G acts on this set by the formula

$$g(aH) = (ga)H, \quad g \in G, \quad aH \in G/H.$$

The mapping $aH \mapsto g(aH)$ will be denoted by $\overline{L}_g$. It is connected with the left shift L_g in G by the formula $\overline{L}_g \circ \omega = \omega \circ L_g$, where ω is a natural mapping $G \to G/H$, $a \mapsto aH$.

Let $\overline{W}$ be the image of W under ω.

According to the foregoing, the mapping $\overline{h}\colon \overline{W} \to \mathbb{R}^{n-m}$ which associates every coset $aH \in \overline{W}$ with a point $\xi \in \mathbb{R}^{n-m}$ for which $a \in V_\xi \cap W$ is correctly defined. Since it is obviously injective and the set $h(\overline{W})$ is an open cube in $\mathbb{R}^{n-m}$ of a half-width c equal to that of W, the pair $(\overline{W}, \overline{h})$ is a chart on G/H containing a point H. That chart is connected

with the chart (W, h) by the commutative diagram

(1)
$$\begin{array}{ccc} W & \longrightarrow & \overline{W} \\ {\scriptstyle h}\downarrow & & \downarrow{\scriptstyle \overline{h}} \\ \mathbb{R}^n & \longrightarrow & \mathbb{R}^{n-m} \end{array}$$

in which the upper horizontal arrow is a mapping ω: $a \mapsto aH$ and the lower one is a projection onto the first m coordinate axes.

By associating every coset $aH \in \overline{W}$, $a \in W$ with a point in W with coordinates

$$x^1 = 0, \ldots, x^m = 0, \qquad x^{m+1} = x^{m+1}(a), \ldots, x^n = x^n(a),$$

we obtain a mapping σ: $\overline{W} \to W$ which is a section of a mapping ω: $W \to \overline{W}$, i.e. such that $\omega \circ \sigma = \text{id}$ on $\overline{W}$. The section σ is connected with mappings h and $\overline{h}$ by the formula

$$\overline{h} = h \circ \sigma.$$

Notice that $\sigma \circ \omega$: $W \to W$ is a smooth mapping.

Since for any element $a \in G$ the mapping $\overline{L}_a$ is bijective, the pair $(a\overline{W}, \overline{h}_a)$, where $\overline{h}_a = \overline{h} \circ \overline{L}_a$, is a chart at $aH \in G/H$. If $a\overline{W} \cap b\overline{W} \neq \varnothing$, then we have for $\overline{h}_b \circ \overline{h}_a^{-1}$ on $h_a(a\overline{W} \cap b\overline{W})$ the formula

$$\begin{aligned} \overline{h}_b \circ \overline{h}_a^{-1} &= \overline{h} \circ \overline{L}_b \circ \overline{L}_a^{-1} \circ \overline{h}^{-1} \\ &= h \circ \sigma \circ \overline{L}_{ba^{-1}} \circ \omega \circ h^{-1} \\ &= h \circ \sigma \circ \omega \circ L_{ba^{-1}} \circ h^{-1} \end{aligned}$$

from which it follows immediately that that mapping is smooth and hence the chart $(a\overline{W}, \overline{h}_a)$ is compatible with a chart $(b\overline{W}, \overline{h}_b)$.

Since charts of the form $(a\overline{W}, \overline{h}_a)$ cover G/H, this proves that they constitute an atlas and therefore define some smoothness on G/H. The set G/H provided with that smoothness is called a *quotient manifold* (or a *homogeneous space*) of a Lie group G mod its closed subgroup H.

The mapping $\omega: G \to G/H$ sends every chart aW to a chart $a\overline{W}$ and therefore (see diagram (1)) is, in the corresponding coordinates, a projection $\mathbb{R}^n \to \mathbb{R}^{n-m}$. This means that a *natural mapping*

$$\omega: G \to G/H, \qquad a \mapsto aH,$$

is smooth and has at all points the same rank $n - m$ (so that its differential $(d\omega)_a$ at every point $a \in G$ is an epimorphism).

The section $\sigma: \overline{W} \to W$ is, of course, a smooth mapping. The mapping

$$\overline{\mu}: G \times G/H \to G/H, \qquad (g, aH) \mapsto (ga)\,H$$

giving the action of the group G on G/H is connected with the multiplication in G by the commutative diagram

$$\begin{tikzcd} G\times G \arrow[r, "\mu"] \arrow[d, "\mathrm{id}\times\omega"'] & G \arrow[d, "\omega"] \\ G\times G/H \arrow[r, "\pi"'] & G/H \end{tikzcd}$$

For any points $g, a \in G$ the mapping id $\times$ ω on a neighbourhood $gW \times a\overline{W}$ of a point (g, aH) has a section id $\times$ σ. On that neighbourhood therefore the mapping $\overline{\mu}$ is a composition of smooth mappings id $\times$ σ, μ, ω and is hence smooth. This proves that $\overline{\mu}$ *is a smooth mapping.*

Suppose now that H is an invariant subgroup. Then the formula

$$aH \cdot bH = abH$$

correctly defines in G/H a multiplication with respect to which G/H is a group. It is easy to see that that multiplication gives a smooth mapping

$$G/H \times G/H \to G/H, \tag{2}$$

i.e. that the *factor group G/H is a Lie group.* Indeed, let $a, b \in G$. Consider neighbourhoods $a\overline{W}$ and $b\overline{W}$ of cosets aH and bH in G/H. On the neighbourhood $a\overline{W} \times b\overline{W}$ mapp-

ing (2) is a composition of smooth mappings $\sigma \times \sigma$, μ, ω and is therefore smooth. Hence it is smooth everywhere. □

Proposition 5. *The Lie algebra of a factor group G/H is isomorphic to a factor algebra of the Lie algebra* $\mathfrak{g} = \mathfrak{l}(G)$ mod *an ideal* $\mathfrak{h} = \mathfrak{l}(H)$:

$$\mathfrak{l}(G/H) \approx \mathfrak{g}/\mathfrak{h}.$$

Proof. Since $\omega\colon G \to G/H$ is a smooth mapping, it is a homomorphism of Lie groups and induces therefore a homomorphism

$$\mathfrak{l}(\omega)\colon \mathfrak{g} \to \mathfrak{l}(G/H)$$

of their Lie algebras. In Lie algebras $\mathfrak{g}$ and $\mathfrak{l}(G/H)$ interpreted as tangent spaces at the point e the homomorphism $\mathfrak{l}(\omega)$ is nothing but a differential

$$(d\omega)_e\colon \mathsf{T}_e(G) \to \mathsf{T}_e(G/H)$$

of ω. But we have seen earlier that that differential is an epimorphism with a kernel $\mathfrak{h} = \mathsf{T}_e(H)$. Therefore, $\mathfrak{l}(\omega)$ induces an isomorphism of a quotient algebra $\mathfrak{g}/\mathfrak{h}$ onto $\mathfrak{l}(G/H)$. □

It should be emphasized that H in this theorem is assumed to be a closed subgroup. Quotient algebras $\mathfrak{g}/\mathfrak{h}$ mod ideals $\mathfrak{h} \subset \mathfrak{g}$ to which there correspond nonclosed invariant subgroups of a Lie group G are not Lie algebra of any factor groups of G (at least if factor groups are understood in the usual sense).

If an invariant subgroup H is not connected, it follows from Proposition 5 that the factor groups G/H and G/H_e, where H_e is the component of the identity of H (which is also an invariant subgroup), are locally isomorphic. This remark can be made more precise if we notice that since $H_e \subset H$ every coset mod H_e is contained in some uniquely defined coset mod H. This fact defines a natural mapping

$$\rho\colon G/H_e \to G/H.$$

Since natural mappings $\omega\colon G \to G/H$ and $\omega_e\colon G \to G/H_e$ are continuous and open, so is ρ. If H is an invariant subgroup, ρ is obviously a homomorphism.

Proposition 6. *For any closed subgroup H of a connected Lie group the natural mapping*

$$\rho\colon G/H_e \to G/H$$

is a covering.

Proof. Since the subgroup H_e is open in a subgroup H, the identity of G has a connected neighbourhood V such that $V^{-1}V \subset H_e$. Proposition 6 will be proved if we show that for any point $\omega(g) = gH$ of the manifold G/H, its neighbourhood $V(g) = \omega(gV)$ is evenly covered by a mapping ρ.

Choosing a representative h_α in every component H_α of H consider in G/H_e open connected sets $\omega_e(gVh_\alpha)$. These, first, do not intersect (if $\omega_e(gvh_\alpha) = \omega_e(gv'h_\beta)$, i.e. $gvh_\alpha = gv'h_\beta h$, where $h \in H_e$, then $h_\alpha = v^{-1}v' \cdot h_\beta h$, where $v^{-1}v' \in H_e$, and therefore $h_\alpha = h_\beta$), second, constitute together the entire set $\rho^{-1}V(g)$ (since cosets of the form gVH, where $v \in V$ are elements of the set $V(g)$, the set $\rho^{-1}V(g)$ consists of cosets of the form $gvh_\alpha H_e$) and, third, ρ maps each of them bijectively, and hence homeomorphically, onto $V(g)$ (if $\omega(gvh_\alpha) = \omega(gv'h_\alpha)$, then $v'h_\alpha = vh_\alpha h$, where $h \in H$ and therefore $v^{-1}v' \in H$ and hence $v^{-1}v' \in H_e$; but then $h = h_\alpha^{-1} \cdot v^{-1}v' \cdot h_\alpha \in H_e$, for H_e is invariant in H, and hence $\omega_e(gvh_\alpha) = \omega_e(gv'h_\alpha)$). Consequently the neighbourhood $V(g)$ is evenly covered by a mapping ρ. □

Corollary. *If under the hypotheses of Proposition* 6 *the quotient manifold* (G/H) *is simply connected, then H is a connected subgroup.* □

We can now show that the general method of establishing the connectedness of topological groups, which relies on Lemma 2 of Lecture 1, can be used to establish simple-connectedness as well:

Proposition 7. *If a connected Lie group G contains a closed connected and simply connected subgroup H* mod *which the quotient manifold G/H is simply connected, then G is also simply connected.*

The following more general proposition is true:

Proposition 8. *Given any connected closed subgroup H of a connected Lie group G* mod *which the quotient manifold G/H is simply connected, fundamental group $\pi_1 G$ of G is a factor group of fundamental group $\pi_1 H$ of the Lie group H.*

Proof. Let $\widetilde{G}$ be a simply connected Lie group covering G and let $\pi: \widetilde{G} \to G$ be the corresponding covering. The complete inverse image $H_\pi = \pi^{-1}H$ of a subgroup H under a homomorphism π is a closed subgroup in $\widetilde{G}$, with the mapping $\widetilde{G}/H_\pi \to G/H$ induced by π being as is easily seen a diffeomorphism. Thus the manifold $\widetilde{G}/H_\pi$ is also simply connected and hence the subgroup H_π is connected. Therefore the restriction π_H of the mapping π to H_π is a covering $H_\pi \to H$ and there is a commutative diagram

$$\begin{tikzcd} \widetilde{H} \arrow[rr] \arrow[dr, "\rho"'] & & H_\pi \arrow[dl, "\pi_H"] \\ & \bar{H} & \end{tikzcd}$$

where $\rho: \widetilde{H} \to H$ is a universal covering of the Lie group H. The mapping $H_\pi \to H$ (being itself a covering) is epimorphic and thus induces an epimorphism of the kernel $\operatorname{Ker} \rho$ of the homomorphism ρ onto the kernel $\operatorname{Ker} \pi_H$ of the homomorphism π_H. This proves Proposition 8 (together with Proposition 7) since by definition $\pi_1 H = \operatorname{Ker} \rho$ and $\pi_1 G = \operatorname{Ker} \pi = \operatorname{Ker} \pi_H$. $\square$

As an example of applying Proposition 7, consider a group SU (n) of unimodular unitary matrices. Since (see Lecture 1) for any $n > 1$ a quotient manifold SU (n)/SU $(n-1)$ = U (n)/U $(n-1)$ is diffeomorphic to a sphere S^{2n-1}, by the corollary to Lemma 1 of Lecture 9 that quotient manifold is simply connected. Since the group SU (1) consists of only one element and is therefore simply connected, by virtue of Proposition 7 an induction leads to the conclusion that *for any* $n \geqslant 1$ *the group* SU (n) *is simply connected.*

A similar reasoning using the simple-connectedness of the sphere $S^{4n-1} = \mathrm{Sp}\,(n)/\mathrm{Sp}\,(n-1)$ and the fact that the group SP (1) $\approx S^3$ is simply connected shows that *given any* $n \geqslant 1$ *the group* Sp (n) = $\mathrm{U}^{\mathbb{H}}$ (n) *is simply connected.*

As for the group U (n) one should apply Proposition 8, since the group U (1), being a group $\mathbb{S}^1$ of complex numbers $|z| = 1$, is not simply connected, for it has a nontrivial covering $\mathbb{R} \to \mathbb{S}^1$ given by the formula $t \mapsto e^{2\pi it}$, $t \in \mathbb{R}$. Since in view of the group $\mathbb{R}$ being simply connected that covering is universal, the group $\pi_1\mathbb{S}^1$ is isomorphic to its kernel, i.e. to the group of integers $\mathbb{Z}$. Therefore the above induction, using, however, Proposition 7 instead of 8, shows that the fundamental group π_1U (n) of a Lie group U (n) is a factor group of the group $\mathbb{Z}$.

To calculate completely that factor group we use the following proposition dual in a certain respect to Proposition 8:

Proposition 9. *For any invariant connected closed subgroup H of a connected Lie group G the fundamental group π_1G/H of the Lie group G/H is a factor group of the fundamental group π_1G of G.*

Proof. Let $\pi\colon \widetilde{G} \to G$ and $\rho\colon \widetilde{G/H} \to G/H$ be universal coverings and let $\omega\colon G \to GH$ be a natural mapping. Since $\widetilde{G}$ is a simply connected group, the homomorphism $\omega \circ \pi\colon \widetilde{G} \to G/H$ is lifted to some homomorphism $\tilde{\omega}\colon \widetilde{G} \to \widetilde{G/H}$. If $\widetilde{H} = \operatorname{Ker} \tilde{\omega}$ and $\tilde{\iota}\colon \widetilde{H} \to \widetilde{G}$ is an embedding, then, with $\omega \circ \pi \circ \tilde{\iota} = \rho \circ \tilde{\omega} \circ \tilde{\iota} = 0$, the homomorphism π sends $\widetilde{H}$ to H and hence induces some homomorphism $\pi_H\colon \widetilde{H} \to H$. All this is graphically represented by the commutative diagram

$$\begin{tikzcd} \widetilde{H} \arrow[r, "\tilde{\iota}"] \arrow[d, "\pi_H"'] & \widetilde{G} \arrow[r, "\tilde{\omega}"] \arrow[d, "\pi"] & \widetilde{G/H} \arrow[d, "\rho"] \\ H \arrow[r, "\iota"'] & G \arrow[r, "\omega"'] & G/H \end{tikzcd}$$

It turns out that if a homomorphism ω is an epimorphism, then it induces an epimorphism of the group $\pi_1G = \operatorname{Ker} \pi$ onto $\pi_1G/H = \operatorname{Ker} \rho$. Indeed, in that case the group $\widetilde{G/H}$

is isomorphic to the factor group $\widetilde{G}/\widetilde{H}$, so that the factor group is a simply connected group. By the corollary to Proposition 6 therefore the subgroup H is connected and hence the homomorphism π_H: $\widetilde{H} \to H$ is a covering and, in particular, an epimorphism. If now $\tilde{a} \in \operatorname{Ker} \rho$ and $\tilde{g}$ is an element in $\widetilde{G}$ such that $\tilde{\omega}(\tilde{g}) = \tilde{a}$, then the element $\pi\tilde{g} \in G$ is in the kernel H of the epimorphism ω and is hence the image under the epimorphism π_H of some element $\tilde{h} \in \widetilde{H}$, i.e. more precisely, we have $(\iota \circ \pi_H)\,\tilde{h} = \pi\tilde{g}$. Then the element $\tilde{g}_1 = (\tilde{\iota}\tilde{h})^{-1}\tilde{g}$ is in the kernel $\operatorname{Ker} \pi$ of a homomorphism π and the given element $\tilde{a} \in \operatorname{Ker} \rho$ is its image $\tilde{\omega}(\tilde{g}_1)$ under the homomorphism $\tilde{\omega}$.

To prove Proposition 9 it is thus sufficient to show that $\tilde{\omega}(\widetilde{G}) = \widetilde{G/H}$.

It is obvious that there are bases $\{U_\alpha\}$ and $\{V_\alpha\}$ of open sets is G and G/H, that consist of connected sets evenly covered by mappings π and ρ respectively, such that for any α the set V_α is the image $\omega(U_\alpha)$ of a set U_α under an epimorphism ω. Let $U_{\alpha,\beta}$ be components of the inverse image $\pi^{-1}(U_\alpha)$ of U_α and $V_{\alpha,\gamma}$ components of the inverse image $\rho^{-1}(V_\alpha)$ of V_α under π and ρ, respectively. Since the homomorphism $\omega \circ \pi$ maps every set $U_{\alpha,\beta}$ onto V_α, the homomorphism $\tilde{\omega}$ maps it onto some set $V_{\alpha,\gamma}$. Therefore, if some set $V_{\alpha,\gamma}$ intersects a subspace $\tilde{\omega}(\widetilde{G})$, then it is contained in that subspace $V_{\alpha,\gamma} \subset \tilde{\omega}(\widetilde{G})$. Since sets of the form $V_{\alpha,\gamma}$ constitute a base of the space $\widetilde{G/H}$, this is possible if any only if $\tilde{\omega}(\widetilde{G})$ is at the same time closed and open. Therefore by connectedness, $\tilde{\omega}(\widetilde{G}) = \widetilde{G/H}$ (cf. the proof of Lemma 3, Lecture 8).

This completes the proof of Proposition 9. $\square$

We apply Proposition 9 to the epimorphism $\mathrm{U}(n) \to S^1$ given by the formula

$$A \mapsto \frac{\det A}{|\det A|}, \qquad A \in \mathrm{U}(n).$$

Since $\pi_1 S^1 = \mathbb{Z}$ the group $\pi_1 \mathrm{U}(n)$ is epimorphically mapped onto the group $\mathbb{Z}$. Since, on the other hand, $\mathbb{Z}$ as shown above, is also epimorphically mapped onto $\pi_1 \mathrm{U}(n)$, this proves that *the fundamental group* $\pi_1 \mathrm{U}(n)$ *of the Lie group* $\mathrm{U}(n)$ *is isomorphic to* $\mathbb{Z}$.

Of the classical connected matrix Lie groups only the group $\mathrm{SO}(n)$ remains to be considered. We shall do this in the next lecture.

Lecture 13

The Clifford algebra of a quadratic functional · *$\mathbb{Z}_2$-graduation of a Clifford algebra* · *More about tensor multiplication of vector spaces and algebras* · *Decomposition of Clifford algebras into a skew tensor product* · *The basis of a Clifford algebra* · *Conjugation in a Clifford algebra* · *The centre of a Clifford algebra* · *A Lie group* Spin (n) · *The fundamental group of a group* SO (n) · *Groups* Spin (n) *with* $n \leqslant 4$ · *Homomorphism* χ · *The group* Spin (6) · *The group* Spin (5) · *Matrix representations of Clifford algebras* · *Matrix representations of groups* Spin (n) · *Matrix groups in which groups* Spin (n) *are represented* · *Reduced representations of groups* Spin (n) · *Additional facts from linear algebra*

We shall begin the calculation of the fundamental group $\pi_1 SO(n)$ of the group SO (n) somewhat from afar.

Let Q be an arbitrary (but fixed once and for all) square functional given in a (finite-dimensional) vector space $\mathscr{V}$ over the field of real numbers $\mathbb{R}$.

We shall consider pairs of the form $(\mathscr{A}, \alpha)$, where $\mathscr{A}$ is a unital algebra over $\mathbb{R}$ (not necessarily finite-dimensional) and α is a linear mapping $\mathscr{V} \to \mathscr{A}$ such that $\alpha(x)^2 = Q(x)1$ for any element $x \in \mathscr{V}$, where 1 is the identity of $\mathscr{A}$. (In what follows, we shall as a rule omit the identity 1 in all equations of this sort, i.e. we shall identify elements of the form $\lambda 1 \in \mathscr{A}$ with the corresponding numbers $\lambda \in \mathbb{R}$.)

Remark 1. To check in practice the condition $\alpha(x)^2 = Q(x)$ it is useful to keep in mind that it holds for all $x \in \mathscr{V}$ if it does for elements of some basis of $\mathscr{V}$.

A *morphism* of a pair $(\mathscr{A}, \alpha)$ into $(\mathscr{B}, \beta)$ is a homomorphism $\Phi\colon \mathscr{A} \to \mathscr{B}$ for which there is a commutative diagram

$$\begin{tikzcd} & \mathscr{V} \arrow[dl, "\alpha"'] \arrow[dr, "\beta"] & \\ \mathscr{A} \arrow[rr, "\Phi"'] & & \mathscr{B} \end{tikzcd}$$

i.e. such a homomorphism that $\beta = \Phi \circ \alpha$. Clearly all pairs $(\mathscr{A}, \alpha)$ and all their morphisms $(\mathscr{A}, \alpha) \to (\mathscr{B}, \beta)$ constitute a category. We shall denote this category by CLIFF (Q).

Recall that an object A_0 of some category G is said to be *initial* (*universal*, in another terminology) if for any object $A \in \mathsf{G}$ there is a unique morphism $A_0 \to A$. Clearly, the initial object (if it exists) is unique up to an isomorphism.

Proposition 1. *There is an initial object in* CLIFF (Q).

Proof. Let

$$\mathsf{T}_0(\mathscr{V}) = \mathsf{T}_0^0(\mathscr{V}) \oplus \ldots \oplus \mathsf{T}_0^q(\mathscr{V}) \oplus \ldots,$$

where $\mathsf{T}_0^q(\mathscr{V})$ is a vector space of multilinear functionals of the $(0, q)$ type in $\mathscr{V}$ (see II, 5). Clearly, with respect to the operation of tensor multiplication, the direct sum $\mathsf{T}_0(\mathscr{V})$ is an (infinite-dimensional) algebra.

In $\mathsf{T}_0(\mathscr{V})$ we consider an ideal $I(Q)$ generated by all elements of the form $\boldsymbol{x} \otimes \boldsymbol{x} - Q(\boldsymbol{x})$, where $\boldsymbol{x} \in \mathscr{V} = \mathsf{T}_0^1(\mathscr{V})$. Let $\mathbb{C}\mathrm{l}(Q)$ is a quotient algebra of $\mathsf{T}_0(\mathscr{V})$ mod the ideal and let $\iota\colon \mathscr{V} \to \mathbb{C}\mathrm{l}(Q)$ a restriction to $\mathscr{V} = \mathsf{T}_0^1(\mathscr{V})$ of the natural epimorphism $\mathsf{T}_0(\mathscr{V}) \to \mathbb{C}\mathrm{l}(Q)$. It turns out that the *pair* $(\mathbb{C}\mathrm{l}(Q), \iota)$ *is the initial object of* CLIFF (Q).

Indeed, by construction, $\iota(\boldsymbol{x})^2 = Q(\boldsymbol{x})$, , so that $(\mathbb{C}\mathrm{l}(Q), \iota) \in$ CLIFF (Q). On the other hand, it is clear that the algebra $\mathsf{T}_0(\mathscr{V})$ is isomorphic to the algebra $\mathbb{R}(x_1, \ldots, x_n)$ of polynomials in n non-commuting unknowns $x_1, \ldots, x_n$ (the isomorphism is defined by a basis $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n$ of $\mathscr{V}$ and realized by the correspondence $\boldsymbol{e}_{i_1} \otimes \ldots \otimes \boldsymbol{e}_{i_q} \mapsto x_{i_1} \ldots x_{i_q}$). For every unital and associative algebra $\mathscr{A}$ therefore, any linear mapping $\alpha\colon \mathscr{V} \to \mathscr{A}$ extends uniquely to some homomorphism $\bar{\alpha}\colon \mathsf{T}_0(\mathscr{V}) \to \mathscr{A}$. If $\alpha(\boldsymbol{x})^2 = Q(\boldsymbol{x}$

for every element $x \in \mathscr{V}$, i.e. if $(\mathscr{A}, \alpha) \in$ CLIFF (Q), then $\bar{\alpha} = 0$ on $I(Q)$ and therefore $\bar{\alpha}$ induces some homomorphism $\alpha_{\#}\colon \mathrm{Cl}(Q) \to \mathscr{A}$ which obviously has the property that $\alpha^{\#} \circ \iota = \alpha$, i.e. which is a morphism $(\mathrm{Cl}(Q), \iota) \to (\mathscr{A}, \alpha)$. Since the vector space $\mathscr{V}$ generates $\mathsf{T}_0(\mathscr{V})$ and hence the vector space $\iota\mathscr{V}$ does the algebra $\mathrm{Cl}(Q)$, the morphism is unique. Consequently the pair $(\mathrm{Cl}(Q), \iota)$ is the initial object of CLIFF (Q). □

Definition 1. The constructed algebra $\mathrm{Cl}(Q)$ is called a *Clifford algebra* of a quadratic functional Q.

By definition, $\mathrm{Cl}(Q)$ has the property that for any object $(\mathscr{A}, \alpha)$ of CLIFF (Q) there is a unique homomorphism of algebras $\alpha^{\#}\colon \mathrm{Cl}(Q) \to \mathscr{A}$ for which $\alpha^{\#} \circ \iota = \alpha$, the algebra $\mathrm{Cl}(Q)$ being completely characterized by this property up to isomorphism.

In the special case, where $\mathscr{V}$ is a Euclidean space and Q is the corresponding metric functional (associating with every vector $x \in \mathscr{V}$ the square of its length, $|x|^2$), the algebra $\mathrm{Cl}(Q)$ will be denoted by $\mathrm{Cl}_+(\mathscr{V})$. But if (on the same assumption that $\mathscr{V}$ is a Euclidean space) the functional Q is defined by the formula $Q(x) = -|x|^2$, then $\mathrm{Cl}(Q)$ will be denoted by $\mathrm{Cl}(\mathscr{V})$. When considered simultaneously, $\mathrm{Cl}_+(\mathscr{V})$ and $\mathrm{Cl}(\mathscr{V})$ will be denoted by $\mathrm{Cl}_\varepsilon(\mathscr{V})$, where $\varepsilon = \pm 1$, meaning the algebra $\mathrm{Cl}_+(\mathscr{V})$ when $\varepsilon = +1$ and the algebra $\mathrm{Cl}(\mathscr{V})$ when $\varepsilon = -1$.

If an orthonormal basis is chosen in $\mathscr{V}$ and thus $\mathscr{V}$ is identified with the standard Euclidean space $\mathbb{R}^n$ we shall denote $\mathrm{Cl}_+(\mathscr{V})$ and $\mathrm{Cl}(\mathscr{V})$ respectively by $\mathrm{Cl}_+(n)$ and $\mathrm{Cl}(n)$ (and by $\mathrm{Cl}_\varepsilon(n)$ when considered simultaneously).

Pairs $(\mathscr{V}, Q)$ form clearly a category $\mathbf{Q}$ whose morphisms $(\mathscr{V}, Q) \to (\mathscr{V}_1, Q_1)$ are linear mappings $\varphi\colon \mathscr{V} \to \mathscr{V}_1$ such that $Q(x) = Q_1(\varphi x)$ for any vector $x \in \mathscr{V}$. Every such mapping obviously induces a homomorphism $\mathsf{T}_0(\mathscr{V}) \to \mathsf{T}_0(\mathscr{V}_1)$ sending an ideal $I(Q)$ to $I(Q_1)$ and hence inducing some homomorphism

$$\mathrm{Cl}\,\varphi\colon \mathrm{Cl}(Q) \to \mathrm{Cl}(Q_1).$$

Clearly, correspondences $(\mathscr{V}, Q) \mapsto \mathrm{Cl}(Q)$, $\varphi \mapsto \mathrm{Cl}\,\varphi$ constitute a functor Cl from the category $\mathbf{Q}$ to the category ALG_0-ASS of associative unit algebras.

Notice that $\mathrm{Cl}\,\varphi$ is nothing but a mapping $(\iota_1 \circ \varphi)^{\#}$, where $\iota_1: \mathscr{V}_1 \to \mathrm{Cl}\,(Q_1)$ is a natural mapping. Allowing a certain liberty we shall use this fact to denote the homomorphism $\mathrm{Cl}\,\varphi$ by $\varphi^{\#}$.

Since $\iota(x)^2 = Q(x)$, it follows from $\iota(x) = \iota(y)$ that $Q(x) = Q(y)$. Therefore the correspondence $\iota(x) \mapsto Q(x)$ correctly defines some square functional in a subspace $\iota\mathscr{V} \subset \mathrm{Cl}\,(Q)$. (In fact, as shown below, it follows from $\iota(x) = \iota(y)$ that $x = y$, so that all these precautions are virtually unnecessary.)

For simplicity we shall denote the functional $\iota(x) \mapsto Q(x)$ as before by Q and the element $\iota(x)$ by x. Accordingly for any element $x \in \iota\mathscr{V}$.

$$x^2 = Q(x). \tag{1}$$

In particular, $(x + y)^2 = Q(x + y)$, i.e. $x^2 + xy + yx + y^2 = Q(x) + 2Q(x, y) + Q(y)$ and hence

$$xy + yx = 2Q(x, y) \tag{2}$$

for any elements $x, y \in \iota\mathscr{V}$.

Let a mapping $-\iota: \mathscr{V} \to \mathrm{Cl}\,(Q)$ be defined by the formula $(-\iota)(x) = -\iota(x)$. Clearly, the pair $(\mathrm{Cl}\,(Q), -\iota)$ is in $\mathrm{CLIFF}\,(Q)$. Therefore a homomorphism $\alpha = (-\iota)^{\#}$ is defined, i.e. a homomorphism $\alpha: \mathrm{Cl}\,(Q) \to \mathrm{Cl}\,(Q)$ having the property that $\alpha x = -x$ if $x \in \iota\mathscr{V}$. Obviously, $\alpha^2 = \mathrm{id}$, i.e. the homomorphism α is an involutory automorphism. For every element $u \in \mathrm{Cl}\,(Q)$, the element αu will be denoted by u^*.

To investigate the automorphism $u \mapsto u^*$ we use the following lemma from linear algebra:

Lemma 1. *If a linear operator $A: \mathscr{W} \to \mathscr{W}$ acting in a real or complex vector space $\mathscr{W}$ is involutory, i.e. if $A^2 = E$, then its eigenvalues are ± 1 and it is diagonalizable, i.e. $\mathscr{W}$ is a direct sum*

$$\mathscr{W} = \mathscr{W}_+ \otimes \mathscr{W}_- \tag{3}$$

of an invariant space $\mathscr{W}_+$ corresponding to the eigenvalue $+1$ and an invariant space $\mathscr{W}_-$ corresponding to the eigenvalue -1.

Proof. Suppose first that the ground field is the field of complex numbers $\mathbb{C}$. Then we can apply to the operator

A the theorem on the reduction to Jordan normal form (see II, 16), i.e. A is a direct sum of operators of the form $\lambda E + C$, where $\lambda \in \mathbb{C}$ and C is either a zero or a cyclic operator. If A is involutory, then each of the operators $\lambda E + C$ is also involutory. But $(\lambda E + C)^2 = \lambda^2 E + 2\lambda C + C^2$ and therefore the equation $(\lambda E + C)^2 = E$ is possible only when $C = 0$. This proves that the original operator A is diagonalizable. Since all elements in an involutory diagonal matrix are obviously ± 1, this completes the proof of Lemma 1 for the case of the ground field $\mathbb{C}$.

If $\mathscr{W}$ is a real space we go over to its complexification $\mathscr{W}^{\mathbb{C}}$ (see II, 17). Since the complexified operator $A^{\mathbb{C}}$ is obviously involutory as before, it follows from the foregoing that

$$\mathscr{W}^{\mathbb{C}} = \mathscr{W}^{\mathbb{C}}_{+} \oplus \mathscr{W}^{\mathbb{C}}_{-}.$$

By restricting ourselves in this decomposition to real vectors we obtain, as is easily seen, precisely decomposition (3). $\square$

By this lemma, as applied to the automorphism $u \mapsto u^*$, the vector space $\mathbb{C}\mathrm{l}\,(Q)$ is decomposed as a direct sum

$$\mathbb{C}\mathrm{l}\,(Q) = \mathbb{C}\mathrm{l}^0\,(Q) \oplus \mathbb{C}\mathrm{l}^1\,(Q)$$

of two subspaces $\mathbb{C}\mathrm{l}^0\,(Q)$ and $\mathbb{C}\mathrm{l}^1\,(Q)$. The elements of $\mathbb{C}\mathrm{l}^0\,(Q)$ are characterized by the condition $u^* = u$ and those of $\mathbb{C}\mathrm{l}^1(Q)$ by the condition $u^* = -u$.

Elements of $\mathbb{C}\mathrm{l}^0\,(Q)$ will be called *even elements* of the Clifford algebra $\mathbb{C}\mathrm{l}\,(Q)$ and those of $\mathbb{C}\mathrm{l}^1\,(Q)$ *odd elements.*

Clearly, a product of two even (odd) elements is even and an odd-even one is odd, i.e.

$$\mathbb{C}\mathrm{l}^i\,(Q) \circ \mathbb{C}\mathrm{l}^j\,(Q) \subset \mathbb{C}\mathrm{l}^{i+j}\,(Q)$$

for any $i, j = 0, 1$ (modulo 2 summation is meant).

In particular, we see that $\mathbb{C}\mathrm{l}^0\,(Q)$ *subspace is a subalgebra of* $\mathbb{C}\mathrm{l}^0(Q)$.

The resulting algebraic structure deserves a special name.

Definition 2. An algebra $\mathscr{A}$ is said to be a $\mathbb{Z}_2$*-graded algebra* if $\mathscr{A} = \mathscr{A}^0 \otimes \mathscr{A}^1$, with

$$\mathscr{A}^i \cdot \mathscr{A}^j \subset \mathscr{A}^{i+j \bmod 2}$$

for any $i, j = 0, 1$. A *morphism* of $\mathbb{Z}_2$-graded algebras is a homomorphism $\varphi: \mathcal{A} \to \mathcal{B}$ such that $\varphi(\mathcal{A}^i) \subset \mathcal{B}^i$ for any $i = 0, 1$. Clearly, all $\mathbb{Z}_2$-graded algebras and all their morphisms constitute a category. The category will be denoted by $\mathbb{Z}_2$-ALG and its subcategory consisting of unital associative algebras by $\mathbb{Z}_2$-ALG$_0$-ASS.

According to the foregoing, the functor $\mathbb{C}\mathrm{l}$ may be assumed to be a functor from the category **Q** to the category $\mathbb{Z}_2$-ALG$_0$-ASS. It is easily seen that if given a pair $(\mathcal{A}, \alpha) \in$ CLIFF (Q) the algebra $\mathcal{A}$ is a $\mathbb{Z}_2$-graded algebra and the mapping $\alpha: \mathcal{V} \to \mathcal{A}$ is a mapping into $\mathcal{A}^1$, then the corresponding homomorphism $\alpha^\#: \mathbb{C}\mathrm{l}(Q) \to \mathcal{A}$ is a morphism of $\mathbb{Z}_2$-graded algebras.

In Lecture 5 we introduced the notion of a product of vector spaces and algebras. Recall that elements of a vector space $\mathcal{A} \otimes \mathcal{B}$ are linear combinations of the form $a \otimes b$, where $a \in \mathcal{A}$ and $b \in \mathcal{B}$, with

$$(a_1 + a_2) \otimes b = a_1 \otimes b + a_2 \otimes b,$$
$$a \otimes (b_1 + b_2) = a \otimes b_1 + a \otimes b_2$$

for any elements $a_1, a_2, a \in \mathcal{A}$ and $b, b_1, b_2 \in \mathcal{B}$. If $e_1, \ldots, e_n$ is a basis of a vector space $\mathcal{A}$ and $f_1, \ldots, f_m$ is a basis of $\mathcal{B}$, then the elements $e_i \otimes f_j$, $i = 1, \ldots, n$, $j = 1, \ldots, m$, constitute a basis of $\mathcal{A} \otimes \mathcal{B}$ (so that, in particular, $\dim(\mathcal{A} \otimes \mathcal{B}) = \dim \mathcal{A} \cdot \dim \mathcal{B}$).

It is immediate from this description of $\mathcal{A} \otimes \mathcal{B}$ that for any vector spaces $\mathcal{A}, \mathcal{B}, \mathcal{C}$ there are natural isomorphisms

(4) $\mathcal{A} \otimes \mathcal{B} \approx \mathcal{B} \otimes \mathcal{A}$ (commutativity),

(5) $(\mathcal{A} \otimes \mathcal{B}) \otimes \mathcal{C} \approx \mathcal{A} \otimes (\mathcal{B} \otimes \mathcal{C})$ (associativity),

(6) $(\mathcal{A} \oplus \mathcal{B}) \otimes \mathcal{C} \approx (\mathcal{A} \otimes \mathcal{C}) \oplus (\mathcal{B} \otimes \mathcal{C})$ (distributivity).

If the spaces $\mathcal{A}$ and $\mathcal{B}$ are algebras we introduce such a multiplication into $\mathcal{A} \otimes \mathcal{B}$ that

$$(a \otimes b)(a_1 \otimes b_1) = aa_1 \otimes bb_1 \tag{7}$$

for any elements $a, a_1 \in \mathcal{A}$, $b, b_1 \in \mathcal{B}$. $\mathcal{A} \otimes \mathcal{B}$ is an algebra with respect to that multiplication and isomorphisms (4), (5) and (6) turn out to be isomorphisms of algebras. (If $\mathcal{A}$ and $\mathcal{B}$ are algebras, then multiplication is introduced

componentwise into the direct sum $\mathcal{A} \oplus \mathcal{B}$, i.e. by the formula $(a, b)(a_1, b_1) = (aa_1, bb_1)$. If $\mathcal{A}$ and $\mathcal{B}$ are associative and unit algebras, then $\mathcal{A} \otimes \mathcal{B}$ is also an associative and unit algebra (with identity element $1 \otimes 1$).

Let $\mathcal{A} = \mathcal{A}^0 \oplus \mathcal{A}^1$ and $\mathcal{B} = \mathcal{B}^0 \oplus \mathcal{B}^1$ be arbirtary $\mathbb{Z}_2$-graded algebras. Then, by putting

$$(\mathcal{A} \otimes \mathcal{B})^0 = (\mathcal{A}^0 \otimes \mathcal{B}^0) \oplus (\mathcal{A}^1 \otimes \mathcal{B}^1),$$
$$(\mathcal{A} \otimes \mathcal{B})^1 = (\mathcal{A}^0 \otimes \mathcal{B}^1) \oplus (\mathcal{A}^1 \otimes \mathcal{B}^0),$$

we immediately get, in view of (4) and (6),

$$\mathcal{A} \otimes \mathcal{B} = (\mathcal{A} \otimes \mathcal{B})^0 \oplus (\mathcal{A} \otimes \mathcal{B})^1.$$

Although the algebra $\mathcal{A} \otimes \mathcal{B}$ is a $\mathbb{Z}_2$-graded algebra with respect to that decomposition, it turns out that it is worthwhile introducing into $\mathcal{A} \otimes \mathcal{B}$ a different multiplication for which

$$(8) \qquad (a \otimes b)(a_1 \otimes b_1) = (-1)^{ij} (aa_1 \otimes bb_1),$$

if $b \in \mathcal{B}^i$ and $a_1 \in \mathcal{A}^j$. It is clear that with respect to that multiplication the vector space $\mathcal{A} \otimes \mathcal{B}$ is also a $\mathbb{Z}_2$-graded algebra, a unit and associative one when so are $\mathcal{A}$ and $\mathcal{B}$.

The algebra $\mathcal{A} \otimes \mathcal{B}$ with multiplication (8) will be called the *skew tensor product* of $\mathbb{Z}_2$-graded algebras $\mathcal{A}$ and $\mathcal{B}$. When it is necessary to stress the difference between this product and the usual (although $\mathbb{Z}_2$-graded) tensor product $\mathcal{A} \otimes \mathcal{B}$ we shall denote it by $\mathcal{A} \hat{\otimes} \mathcal{B}$.

The three tensor multiplications (for vector spaces, for algebras and for $\mathbb{Z}_2$-graded algebras) all have the property of being functorial, i.e. for any morphisms $\varphi: \mathcal{A} \to \mathcal{A}_1$, $\psi: \mathcal{B} \to \mathcal{B}_1$ a morphism $\varphi \otimes \psi: \mathcal{A} \otimes \mathcal{B} \to \mathcal{A}_1 \otimes \mathcal{B}_1$ is defined which satisfied the usual functorial identities. That morphism is uniquely characterized by the relation

$$(\varphi \otimes \psi)(a \otimes b) = \varphi(a) \otimes \psi(b),$$

which must hold for any elements $a \in \mathcal{A}$, $b \in \mathcal{B}$.

In addition, for any vector spaces $\mathcal{A}$ and $\mathcal{B}$ and any algebra $\mathcal{C}$ we can associate with linear mappings $\varphi: \mathcal{A} \to \mathcal{C}$ and $\psi: \mathcal{B} \to \mathcal{C}$ a linear mapping $\varphi \otimes \psi: \mathcal{A} \otimes \mathcal{B} \to \mathcal{C}$ which is uniquely characterized by the relation

$$(\varphi \otimes \psi)(a \otimes b) = \varphi(a)\psi(b), \quad a \in \mathcal{A}, \qquad b \in \mathcal{B}.$$

If $\mathcal{A}$ and $\mathcal{B}$ are algebras and $\varphi\colon \mathcal{A} \to \mathcal{C}$ and $\psi\colon \mathcal{B} \to \mathcal{C}$ are homomorphisms, with φ and ψ *commuting* (i.e. $\varphi a \cdot \psi b = \psi b \cdot \varphi a$ for any elements $a \in \mathcal{A}$ and $b \in \mathcal{B}$), then the mapping $\varphi \otimes \psi\colon \mathcal{A} \otimes \mathcal{B} \to \mathcal{C}$ is also a homomorphism. Similarly, for any $\mathbb{Z}_2$-graded algebras $\mathcal{A}$, $\mathcal{B}$ and $\mathcal{C}$ and any *skew commutative* morphisms $\varphi\colon \mathcal{A} \to \mathcal{C}$ and $\psi\colon \mathcal{B} \to \mathcal{C}$ (i.e. such that $\varphi a \cdot \psi b = (-1)^{ij} \psi b \cdot \varphi a$ if $a \in \mathcal{A}^i$, $b \in \mathcal{B}^j$) the mapping $\varphi \otimes \psi\colon \mathcal{A} \otimes \mathcal{B} \to \mathcal{C}$ is a morphism of a skew tensor product $\mathcal{A} \hat{\otimes} \mathcal{B}$ into the algebra $\mathcal{C}$.

For every two objects $(\mathcal{V}_1, Q_1)$ and $(\mathcal{V}_2, Q_2)$ of $\mathbf{Q}$ the formula

$$Q(\boldsymbol{x}_1 + \boldsymbol{x}_2) = Q_1(\boldsymbol{x}_1) + Q_2(\boldsymbol{x}_2), \quad \boldsymbol{x}_1 \in \mathcal{V}_1, \quad \boldsymbol{x}_2 \in \mathcal{V}_2,$$

defines on the direct sum $\mathcal{V} = \mathcal{V}_1 \otimes \mathcal{V}_2$ a quadratic functional Q called the *direct sum* of quadratic functionals Q_1 and Q_2 (and usually denoted by $Q_1 \oplus Q_2$).

In these terms the *Lagrange theorem* (see II, 11) means that any quadratic functional is a direct sum of functionals in one-dimensional spaces.

Proposition 2. *For any two quadratic functionals Q_1 and Q_2 there is a natural isomorphism*

$$\mathrm{Cl}(Q_1 \oplus Q_2) \approx \mathrm{Cl}(Q_1) \widehat{\otimes} \mathrm{Cl}(Q_2).$$

Proof. Putting $\mathcal{V} = \mathcal{V}_1 \oplus \mathcal{V}_2$ define a linear mapping

$$\alpha\colon \quad \mathcal{V} \to \mathrm{Cl}(Q_1) \widehat{\otimes} \mathrm{Cl}(Q_2)$$

by the formula

$$\alpha(\boldsymbol{x}_1 + \boldsymbol{x}_2) = x_1 \otimes 1 + 1 \otimes x_2, \qquad (9)$$
$$\boldsymbol{x}_1 \in \mathcal{V}_1, \ \boldsymbol{x}_2 \in \mathcal{V}_2,$$

where as ever $x_1 = \iota \boldsymbol{x}_1$, $x_2 = \iota \boldsymbol{x}_2$. Since

$$(x_1 \otimes 1)(1 \otimes x_2) = x_1 \otimes x_2$$

and

$$(1 \otimes x_2)(x_1 \otimes 1) = -(x_1 \otimes x_2),$$

we have

$$\begin{aligned} \alpha(x)^2 = \alpha(\boldsymbol{x}_1 + \boldsymbol{x}_2)^2 &= (x_1 \otimes 1 + 1 \otimes x_2)^2 \\ &= x_1^2 \otimes 1 + 1 \otimes x_2^2 \\ &= Q_1(\boldsymbol{x}_1) + Q_2(\boldsymbol{x}_2) = Q(\boldsymbol{x}) \end{aligned}$$

for any vector $x = x_1 + x_2 \in \mathscr{V}$, where $x_1 \in \mathscr{V}_1$, $x_2 \in \mathscr{V}_2$, $Q = Q_1 \oplus Q_2$ and hence $(\mathrm{Cl}\,(Q_1) \,\hat{\otimes}\, \mathrm{Cl}\,(Q_2),\ \alpha) \in \mathrm{CLIFF}\,(Q)$. We show that the *corresponding morphism*

$$\alpha^{\#}\colon \mathrm{Cl}\,(Q) \to \mathrm{Cl}\,(Q_1) \,\hat{\otimes}\, \mathrm{Cl}\,(Q_2)$$

of $\mathbb{Z}_2$-graded algebras is an isomorphism.

To this end we consider natural embeddings $\sigma_1\colon \mathscr{V}_1 \to \mathscr{V}$ and $\sigma_2\colon \mathscr{V}_2 \to \mathscr{V}$. These are clearly morphisms of pairs $(\mathscr{V}_1, Q_1)$ and $(\mathscr{V}_2, Q_2)$ into $(\mathscr{V}, Q)$, respectively. Therefore homomorphisms $\sigma_1^{\#}\colon \mathrm{Cl}\,(Q_1) \to \mathrm{Cl}\,Q$ and $\sigma_2^{\#}\colon \mathrm{Cl}\,(Q_2) \to \mathrm{Cl}\,(Q)$ are defined. Since for any vectors $x_1 \in \mathscr{V}_1$ and $x_2 \in \mathscr{V}_2$ the vectors $\sigma_1 x_1, \sigma_2 x_2 \in \mathscr{V}$ are by definition Q-orthogonal, by formula (2)

$$\sigma_1^{\#} x_1 \cdot \sigma_2^{\#} x_2 = -\sigma_2^{\#} x_2 \cdot \sigma_1^{\#} x_1.$$

Since any even (odd) element of the algebra $\mathrm{Cl}\,(Q_i)$, $i = 1, 2$, is the sum of the products of an even (odd) number of elements $x_i \in \iota\mathscr{V}_i$, it follows immediately that mappings $\sigma_1^{\#}$ and $\sigma_2^{\#}$ are skew commutative and therefore the mapping $\sigma_1^{\#} \otimes \sigma_2^{\#}\colon \mathrm{Cl}\,(Q_1) \,\hat{\otimes}\, \mathrm{Cl}\,(Q_2) \to \mathrm{Cl}\,(Q)$ is a morphism of $\mathbb{Z}_2$-graded algebra $\mathrm{Cl}\,(Q_1) \,\hat{\otimes}\, \mathrm{Cl}\,(Q_2)$ into $\mathbb{Z}_2$-graded algebra $\mathrm{Cl}\,(Q)$.

In accurate notation (with σ_1 and σ_2) formula (9) is of the form

$$\alpha\,(\sigma_1 x_1 + \sigma_2 x_2) = x_1 \otimes 1 + 1 \otimes x_2.$$

Since by definition $\sigma_1^{\#} x_1 = \iota\sigma_1 x_1$, $\sigma_2^{\#} x_2 = \iota\sigma_2 x_2$ and $\alpha^{\#} \circ \iota = \alpha$, it follows that

$$\alpha^{\#}(\sigma_1^{\#} x_1 + \sigma_2^{\#} x_2) = x_1 \otimes 1 + 1 \otimes x_2$$

for any elements $x_1 \in \iota\mathscr{V}_1$ and $x_2 \in \iota\mathscr{V}_2$. Here $\sigma_1^{\#} x_1 + \sigma_2^{\#} x_2$ is nothing but an element x of $\iota\mathscr{V}$. Therefore

$$\begin{aligned}((\sigma_1^{\#} \otimes \sigma_2^{\#}) \circ \alpha^{\#})\, x &= (\sigma_1^{\#} \otimes \sigma_2^{\#})\,(x_1 \otimes 1 + 1 \otimes x_2)\\ &= \sigma_1^{\#} x_1 \cdot 1 + 1 \cdot \sigma_2^{\#} x_2\\ &= \sigma_1^{\#} x_1 + \sigma_2^{\#} x_2 = x,\end{aligned}$$

so that $(\sigma_1^{\#} \otimes \sigma_2^{\#}) \circ \alpha^{\#} = \mathrm{id}$ in the subspace $\iota\mathscr{V}$. Since the mapping $(\sigma_1^{\#} \otimes \sigma_2^{\#}) \circ \alpha^{\#}$ is a homomorphism of algebras while

$\iota\mathscr{V}$ generates the algebra $\mathrm{Cl}\,(Q)$, it follows that $(\sigma_1^\# \otimes \sigma_2^\#) \circ \alpha^\# = \mathrm{id}$ on the entire algebra $\mathrm{Cl}\,(Q)$.
Similarly

$$(\alpha^\# \circ (\sigma_1^\# \otimes \sigma_2^\#))\,(x_1 \otimes 1) = \alpha^\#\,(\sigma_1^\# x_1 \cdot 1) = x_1 \otimes 1$$
$$(\alpha^\# \circ (\sigma_1^\# \otimes \sigma_2^\#))\,(1 \otimes x_2) = \alpha^\#\,(1 \cdot \sigma_2^\# x_2) = (1 \otimes x_2)$$

for any elements $x_1 \in \iota\mathscr{V}_1$, $x_2 \in \iota\mathscr{V}_2$ and hence $\alpha^\# \circ (\sigma_1^\# \otimes \sigma_2^\#) = \mathrm{id}$ since the elements $x_1 \otimes 1$, $x_1 \in \iota\mathscr{V}_1$ and $1 \otimes x_2$, $x_2 \in \iota\mathscr{V}_2$, generate the algebra $\mathrm{Cl}\,(Q_1) \mathbin{\hat{\otimes}} \mathrm{Cl}\,(Q_2)$.

Thus morphisms $\alpha^\#$ and $\sigma_1^\# \otimes \sigma_2^\#$ are inverse isomorphisms. □

Let $n = \dim \mathscr{V}$. Given $n = 1$ there are (up to isomorphism) only three quadratic functionals Q_{+1}, Q_{-1} and Q_0 characterized by assuming the values $+1$, -1 and 0, respectively on some vector $e \in \mathscr{V}$ (which is the basis of a one-dimensional space $\mathscr{V}$). Since for $n = 1$ the algebra $\mathsf{T}_0\,(\mathscr{V})$ is isomorphic to the algebra $\mathbb{R}\,[e]$ of (usual) polynomials in e, it follows that the algebra $\mathrm{Cl}\,(Q_\varepsilon)$, $\varepsilon = \pm 1$, 0 is obtained from $\mathbb{R}\,[e]$ by superposing the relation $e^2 = \varepsilon$, i.e. it is the algebra $\mathbb{C}$ of complex numbers or the algebra $\mathbb{D}$ of *double numbers* (of the form $a + be$, where a, $b \in \mathbb{R}$ and $e^2 = 1$) or the algebra of *dual numbers* (of the form $a + be$, where a, $b \in \mathbb{R}$ and $e^2 = 0$).

Theorem 1. *For any quadratic functional Q in an n-dimensional space $\mathscr{V}$ the Clifford algebra $\mathrm{Cl}\,(Q)$ is isomorphic to a skew tensor product of p algebras of double numbers, $r - p$ algebras of complex numbers and $n - r$ algebras of dual numbers, where r is the rank of the functional Q and p is its positive index of inertia. In particular,*

$$\mathrm{Cl}\,(n) = \underbrace{\mathbb{C} \mathbin{\hat{\otimes}} \ldots \mathbin{\hat{\otimes}} \mathbb{C}}_{n \text{ times}}, \quad \mathrm{Cl}_+\,(n) = \underbrace{\mathbb{D} \mathbin{\hat{\otimes}} \ldots \mathbin{\hat{\otimes}} \mathbb{D}}_{n \text{ times}}.$$

Proof. It can be obtained by induction from Proposition 2 and Lagrange's theorem. □

Since under tensor multiplication the dimensions of quotient algebras are multiplied out, it follows from Theorem 1 in particular that $\dim \mathrm{Cl}\,(Q) = 2^n$.

Moreover, if $e_1, \ldots, e_n$ is a Q-orthogonal basis of a space $\mathscr{V}$, then, the basis of the ith factor consisting of elements 1 and e_i, the algebra $\mathrm{Cl}\,(Q)$ has a basis consisting of 2^n elements of the form $x_{k_1}^{(1)}x_{k_2}^{(2)} \ldots x_{k_n}^{(n)}$, where $k_1, k_2, \ldots, k_n = 0, 1$ and $x_0^{(i)} = 1$ and $x_1^{(i)} = e_i$ for any $i = 1, \ldots, n$.

On introducing a subset I of an interval $[n] = \{1, 2, \ldots, n\}$ of a natural series, the subset consisting of indices i for which $k_i = 1$, we shall denote an element $x_{k_1}^{(1)}x_{k_2}^{(2)} \ldots x_{k_n}^{(n)}$ by e_I. Thus if $I = \{i_1 < i_2 < \ldots < i_m\}$, then $e_I = e_{i_1} \ldots e_{i_m}$.

The number m will be denoted by $|I|$.

In particular, for $m = 1$ we obtain elements $e_{\{1\}} = e_1, \ldots, e_{\{n\}} = e_n$. Therefore *these elements are linearly independent* and hence the linear mapping $\iota\colon \mathscr{V} \to \mathrm{Cl}\,(Q)$ (recall that it sends the basis vectors $e_1, \ldots, e_n$ to elements $e_1, \ldots, e_n$) is precisely a monomorphism, as was stated above. As a rule we shall identify every vector $x \in \mathscr{V}$ with the corresponding element $x \in \iota\mathscr{V} \in \mathrm{Cl}\,(Q)$. By this convention, the morphism $\alpha^\#\colon \mathrm{Cl}\,(Q) \to \mathscr{A}$ for any object $(\mathscr{A}, \alpha) \in \mathrm{CLIFF}\,(Q)$ will be nothing but an extension of the mapping α from $\mathscr{V}$ to $\mathrm{Cl}\,(Q)$.

For $m = 0$, i.e. for $I = \varnothing$, the element $e_\varnothing$ (denoted also by e_0) is the identity 1 of the algebra $\mathrm{Cl}\,(Q)$.

Since the vectors e_i and e_j are by hypothesis Q-orthogonal, it follows from (2) that

$$e_ie_j + e_je_i = 0, \quad i \neq j. \tag{10}$$

In addition, by formula (1)

$$e_i^2 = \varepsilon_i \text{ where } \varepsilon_i = Q\,(e_i). \tag{11}$$

Relations (10) and (11) allow a product of any basis elements e_I and e_J to be immediately written. For example, for $n = r$ and $p = 0$, i.e. in $\mathrm{Cl}_+\,(n)$, we have the formula

$$e_Ie_J = (-1)^{\tau_+(I,J)}e_{I\Delta J}, \tag{12}$$

where $I\Delta J = (I \cup J)\setminus(I \cap J)$ is a symmetric difference of the sets I and J and $\tau_+\,(I, J)$ is the number of all pairs $(i, j) \in I \times J$ for which $i > j$.

Similarly in $\mathbb{C}\mathrm{l}\,(n)$

(13) $$e_I e_J = (-1)^{\tau(I,\,J)} e_{I\Delta J},$$

where $\tau\,(I,\ J)$ is the number of pairs $(i,\ j) \in I \times J$ such that $i \geqslant j$.

A linear mapping $a \mapsto \bar{a}$ of a not necessarily associative algebra $\mathcal{A}$ into itself is said to be an *involutory antiautomorphism* if $\bar{\bar{a}} = a$ and $\overline{ab} = \bar{b}\bar{a}$ for any elements $a,\ b \in \mathcal{A}$. An example is a mapping of a tensor algebra $\mathsf{T}_0\,(\mathscr{V})$ into itself that is given on generators $x_1 \otimes \ldots \otimes x_p$ by the formula

$$\overline{x_1 \otimes \ldots \otimes x_p} = x_p \otimes \ldots \otimes x_1.$$

Since all elements of the form $x \otimes x - Q\,(x)$ remain fixed under this antiautomorphism, $\overline{I\,(Q)} = I\,(Q)$ and therefore the antiautomorphism induces some involutory antiautomorphism of the algebra $\mathbb{C}\mathrm{l}\,(Q)$.

Definition 3. The involutory antiautomorphism $a \mapsto \bar{a}$ of $\mathbb{C}\mathrm{l}\,(Q)$ is called a *conjugation*.

On the basis elements e_I, $I = \{i_1 < \ldots < i_m\} \subset [n]$ the conjugation acts, as is easily seen, by the formula

$$\bar{e}_I = (-1)^{\frac{m(m-1)}{2}} e_I.$$

Thus $\bar{e}_I = e_I$ when $m = 4p,\ 4p + 1$, and $\bar{e}_I = -e_I$ when $m = 4p + 2,\ 4p + 3$.

Recall that the *centre* of an associative algebra is its subalgebra consisting of all elements commutative with each element of the algebra.

We calculate the centre of the Clifford algebra $\mathbb{C}\mathrm{l}\,(Q)$ for the case where the functional Q is positively or negatively defined, i.e. for algebras $\mathbb{C}\mathrm{l}_\varepsilon\,(n)$.

Proposition 3. *If n is even, then the centre of an algebra $\mathbb{C}\mathrm{l}_\varepsilon\,(n)$ is one-dimensional (and consists only of the elements of $\mathbb{R}$) but if n is odd, then the centre of $\mathbb{C}\mathrm{l}_\varepsilon\,(n)$ is two-dimensional and is generated by the elements* 1 *and* $e_{[n]} = e_1 e_2 \ldots e_n$.

Proof. Since the elements $e_1, \ldots, e_n$ generate an algebra $\mathbb{C}\mathrm{l}_\varepsilon\,(n)$, every element $x \in \mathbb{C}\mathrm{l}_\varepsilon\,(n)$ is in the centre of that algebra if and only if $xe_i = e_i x$, i.e. $e_i x e_i = \varepsilon x$, for any

$i = 1, \ldots, n$. Clearly, if $i \in I = \{i_1 < \ldots < i_m\}$ and $i = i_t$, then

$$e_i e_I = (-1)^{t-1} \varepsilon e_{I\setminus\{i\}} \text{ and}$$
$$e_I e_i = (-1)^{m-t} \varepsilon e_{I\setminus\{i\}},$$

and if $i \notin I$ and $i_{t-1} < i < i_t$, then

$$e_i e_I = (-1)^{t-1} e_{I\cup\{i\}} \text{ and}$$
$$e_I e_i = (-1)^{m-t+1} e_{I\cup\{i\}}.$$

Therefore if $x = \sum_I x_I e_I$, then

$$e_i x e_i = \sum_{i\in I} (-1)^{m+1} \varepsilon x_I e_I + \sum_{i\notin I} (-1^m) \varepsilon x_I e_I, \text{ where } m = |I|.$$

Hence $e_i x e_i = \varepsilon x_i$ if and only if $x_I = (-x)^{m+1} x_I$ for $i \in I$ and $x_I = (-1)^m x_I$ for $i \notin I$. Since given any $I \neq \varnothing$ $[n]$ exists as both $i \in I$ and $i \notin I$, it follows that if $e_i x e_i = \varepsilon x$ for all $i = 1, \ldots, n$, then $(-1)^{m+1} x_I = (-1)^m x_I$ and hence $x_I = 0$. Besides $x_{[n]} = (-1)^{n+1} x_{[n]}$ and hence $x_{[n]} = 0$ if n is even. Therefore $x = x_\varnothing e_\varnothing$ if n is even and $x = x_\varnothing e_\varnothing + x_{[n]} e_{[n]}$ if n is odd. □

Corollary. *For any n and any ε numbers in $\mathbb{R}$ are the only even elements of the centre of an algebra* $\mathrm{Cl}_\varepsilon(n)$. □

Since $x^2 = \varepsilon |x|^2$ for every element $x \in \iota\mathbb{R}^n = \mathbb{R}^n$, all nonzero elements of $\mathbb{R}^n$ are invertible in $\mathrm{Cl}_\varepsilon(n)$. In particular, so are all elements in a unit sphere S^{n-1} of a space $\mathbb{R}^n$ with $x^{-1} = \varepsilon x = \bar{\varepsilon x}$ if $x \in S^{n-1}$.

Definition 4. A subgroup $\mathrm{pin}_\varepsilon(n)$ of the multiplicative group of all invertible elements of an algebra $\mathrm{Cl}_\varepsilon(n)$ which is generated by elements of S^{n-1} is called a *Clifford group* of degree n and index ε. This group is also denoted by $\mathrm{pin}_+(n)$ if $\varepsilon = -1$.

A subgroup of $\mathrm{pin}_\varepsilon(n)$ consisting of even elements is denoted by $\mathrm{Spin}_\varepsilon(n)$ (and also by $\mathrm{Spin}_+(n)$ if $\varepsilon = +1$ and by $\mathrm{Spin}(n)$ if $\varepsilon = -1$) and called a *spinor group* of degree n and index ε.

Clearly, groups $\mathrm{pin}_\varepsilon(n)$ and $\mathrm{Spin}_\varepsilon(n)$ are closed in the Lie group of all invertible elements of $\mathrm{Cl}_\varepsilon(n)$. Therefore these groups are Lie groups.

By definition, every element u of $\mathrm{pin}_\varepsilon(n)$ can be represented (not uniquely in general) as a product $x_1 \ldots x_m$, where $x_1, \ldots, x_m \in S^{n-1}$, and the element is in $\mathrm{Spin}_\varepsilon(n)$ if and only if m is even. Since both $u \mapsto u^{-1}$ and $u \mapsto \bar{u}$ mappings are antiautomorphisms and $x^{-1} = \varepsilon\bar{x}$ for $x \in S^{n-1}$, we have $u^{-1} = \varepsilon^m\bar{u}$ and hence

$$u^{-1} = \bar{u} \text{ if } u \in \mathrm{Spin}_\varepsilon(n) \text{ (or } \varepsilon = +1).$$

If

$$u = \sum_{i=1}^{n} u_i e_i \in \mathbb{R}^n \text{ and } x = \sum_{i=1}^{n} x_i e_i \in \mathbb{R}^n,$$

$$ux = -\sum_{i=1}^{n} u_i x_i + \sum_{i \neq j} u_i x_j e_i e_j,$$

and hence

$$ux\bar{u} = \sum_{(ijk)} u_i x_j u_k e_i e_j e_k + \ldots,$$

where the dots signify terms linear in $e_1, \ldots, e_n$ (i.e. terms in $\mathbb{R}^n$) and (ijk) under the summation sign designates that the summation is taken over all triples (ijk) consisting of pairwise distinct numbers $1, \ldots, n$. Interchanging any factors makes the product $e_i e_j e_k$ change sign and the coefficients $u_i x_j u_k$ are symmetric in i and k. Therefore the sum is zero and hence $ux\bar{u} \in \mathbb{R}^n$. Since $(uv)\, x\, (\overline{uv}) = u\,(vx\bar{v})\,\bar{u}$, $ux\bar{u} \in \mathbb{R}^n$ for any element $u \in \mathrm{Cl}\,(n)$ representable as a product of elements of $\mathbb{R}^n$ and hence, in particular, for any element $u \in \mathrm{pin}_\varepsilon(n)$. This shows that by putting

$$\varphi\,(u)\, x = ux\bar{u}, \quad u \in \mathrm{pin}_\varepsilon(n), \quad x \in \mathbb{R}^n,$$

we obtain some (obviously linear) mapping

$$\varphi\,(u)\colon \quad \mathbb{R}^n \to \mathbb{R}^n.$$

We also see that $\varphi\,(uv) = \varphi\,(u)\,\varphi\,(v)$, i.e. that $\varphi\colon u \mapsto \varphi\,(u)$ is a homomorphism of a group $\mathrm{pin}_\varepsilon\,(n)$ into a group of invertible linear operators $\mathbb{R}^n \to \mathbb{R}^n$ which, using the fact that we have a fixed basis $e_1, \ldots, e_n$ in $\mathbb{R}^n$ will be identified with a group $\mathrm{GL}\,(n)$ of invertible matrices.

Moreover, since for every element $x \in \mathbb{R}^n$

$$| \varphi (u) x |^2 = \varepsilon (\varphi (u) x)^2 = \varepsilon ux\bar{u}ux\bar{u}$$
$$= \varepsilon uxu^{-1}uxu^{-1} = \varepsilon uxxu^{-1} = | x |^2uu^{-1} = | x |^2,$$

the operator $\varphi (u)$ for any element $u \in \mathrm{pin}_\varepsilon(u)$ is orthogonal, so that φ is indeed a homomorphism

$$\varphi\colon \mathrm{pin}_\varepsilon (n) \to \mathrm{O} (n).$$

Proposition 4. *The mapping*

$$\varphi\colon \mathrm{pin}_\varepsilon(n) \to \mathrm{O} (n),$$

with $\varepsilon = -1$ *or* n *even, is an epimorphism onto a group* $\mathrm{O}(n)$ *and, with* $\varepsilon = +1$ *and* n *odd, it is an epimorphism onto a group* $\mathrm{SO}(n)$.

Given any ε *and* n *the homomorphism* φ *maps a group* $\mathrm{Spin}_\varepsilon (n)$ *into* $\mathrm{SO} (n)$, *with the induced homomorphism*

$$\varphi_1\colon \mathrm{Spin}_\varepsilon(n) \to \mathrm{SO} (n)$$

being an epimorphism.

The second-order group $\{1, -1\}$ *is the kernel of the epimorphism* φ_0.

Proof. If $u \in S^{n-1}$ and $x \in \mathbb{R}^n$, then by formula (2)

$$\varphi (u) x = ux\bar{u} = uxu = (2\varepsilon (x, u) - xu) u$$
$$= -\varepsilon (x - 2 (x, u) u)$$

and hence

$$\varphi (u) = -\varepsilon u^\perp,$$

where $u^\perp\colon x \mapsto x - 2 (x, u) u$ is a symmetry in the hyperplane perpendicular to a vector u. Therefore any symmetry of $\mathbb{R}^n$ (when $\varepsilon = -1$) and a composition of a symmetry and the operator $x \mapsto -x$ with the determinant $(-1)^n$ (when $\varepsilon = 1$) is in the image of the homomorphism φ. This proves the first three statements of Proposition 4. Indeed, we know (see I, 27) that in one- and two-dimensional spaces any orthogonal operator is a symmetry or a composition of symmetries, and in an n-dimensional space it is a direct sum of orthogonal operators in one- and two-dimensional subspaces (see II, 21) and hence again a symmetry or a composition of symmetries. The operator is in

SO (n) if and only if it is a composition of an even number of symmetries.

If $u \in \operatorname{Ker} \varphi_0$ then $ue_i = e_i u$ for any $i = 1, \ldots, n$ (for, as observed above, $u^{-1} = \bar{u}$ for any element $u \in \mathrm{Spin}_\varepsilon(n)$ and hence u is in the centre of $\mathrm{Cl}_\varepsilon(n)$, i.e. being odd, it is a number in $\mathbb{R}$. Therefore $\varphi(u)\,x = u^2 x$, i.e. $\varphi(u) = u^2 E$ and consequently, with the operator $\varphi(u)$ being orthogonal, $u = \pm 1$. Conversely, it is clear that $\pm 1 \in \operatorname{Ker} \varphi_0$. $\square$

It follows from Proposition 4 that if for $n > 1$ the Lie group $\mathrm{Spin}_\varepsilon(n)$ is connected, then the epimorphism φ_0 is a group covering. Otherwise $\mathrm{Spin}_\varepsilon(n)$ must be a direct product $\mathrm{SO}(n) \times \mathbb{Z}_2$ (and the mapping φ_0 must be a projection $\mathrm{SO}(n) \times \mathbb{Z}_2 \to \mathrm{SO}(n)$) and hence the points 1 and -1 of Spin (n) will be in distinct components of the group. But it is obvious that if we put

$$\begin{aligned} u(t) &= \varepsilon\left(\cos\frac{\pi}{2}t\cdot e_1 + \sin\frac{\pi}{2}t\cdot e_2\right) \\ &\quad\times\left(\cos\frac{\pi}{2}t\cdot e_1 - \sin\frac{\pi}{2}t\cdot e_2\right) \\ &= \cos\pi t - \varepsilon\sin\pi t\cdot e_1e_2, \quad 0 \leqslant t \leqslant 1, \end{aligned}$$

we obtain in $\mathrm{Spin}_\varepsilon(n)$ a path $t \mapsto u(t)$ connecting the point 1 with -1. Therefore the first case must take place. Consequently, the *group* $\mathrm{Spin}_\varepsilon(n)$ *with* $n > 1$ *is connected and the epimorphism* φ_0 *is a group covering.*

The inverse image of any point for the covering φ_0 consists of two elements. This kind of covering is called a *two-sheeted* (*or double*) covering.

The fact that SO (n) has a nontrivial covering implies that SO (n) *is not simply connected.*

To find its fundamental group we again use Proposition 8 of Lecture 12. As already observed in Lecture 1, the quotient manifold $\mathrm{SO}(n)/\mathrm{SO}(n-1)$ is naturally identified with a sphere S^{n-1} and is therefore simply connected for $n \geqslant 3$. By Proposition 8 of Lecture 12, therefore, for any $n \geqslant 3$ the fundamental group $\pi_1\mathrm{SO}(n)$ of SO (n) is the factor group of the group $\pi_1\mathrm{SO}(3)$. It is therefore sufficient for us to calculate only the group $\pi_1\mathrm{SO}(3)$.

Let $\mathbb{H}'$ be a vector space of "pure imaginary" quaternions η (i.e. such that $\overline{\eta} = -\eta$) and S^3 be a group of "unit" quaternions ξ (i.e. such that $\overline{\xi} = \xi^{-1}$). If $\xi = S^3$ and $\eta \in \mathbb{H}'$, then $\overline{\xi\eta\xi^{-1}} = \overline{\xi^{-1}}\,\overline{\eta}\,\overline{\xi} = -\xi\eta\xi^{-1}$ and hence $\xi\eta\xi^{-1} \in \mathbb{H}'$. Consequently, for any quaternion $\xi \in S^3$ the formula $\varphi(\xi)\colon \eta \mapsto \xi\eta\xi^{-1}$, $\eta \in \mathbb{H}'$, defines an (obviously linear) operator $\varphi(\xi)\colon \mathbb{H}' \to \mathbb{H}'$. Since $|\xi\eta\xi^{-1}| = |\eta|$, the operator $\varphi(\xi)$ is orthogonal. By virtue of the identification $\mathbb{H}' = \mathbb{R}^3$ the mapping $\varphi\colon \xi \mapsto \varphi(\xi)$ is therefore a mapping (obviously homomorphous) of the group S^3 into O (3). Moreover, since S^3 is a connected group, the homomorphism φ is in fact a mapping into SO (3).

Proposition 5. The *homomorphism*

$$\psi\colon S^3 \to \mathrm{SO}\ (3)$$

is an epimorphism. The second-order group $\{1, -1\}$ *i, its kernel.*

We shall use the following general lemma to prove this proposition.

Lemma 2. *A homomorphism* $\Phi\colon G \to H$ *of connected Lie groups is a group covering (and hence an epimorphism) if its kernel* $K = \operatorname{Ker}\Phi$ *is discrete and* $\dim G = \dim H$.

Proof. Since the kernel of Φ is discrete, the homomorphism considered as a mapping onto its image $\Phi(G) \approx G/K$ is a group covering. Therefore it is only necessary to prove that $\Phi(G) = H$. Since $\dim \Phi(G) = \dim(G) = \dim H$, the identity $e \in \Phi(G)$ is an interior point of the subgroup $\Phi(G)$, i. e. there is a neighbourhood of the identity U in H, such that $U \subset \Phi(G)$. This proves the lemma since by virtue of the connectedness of the group H the neighbourhood U generates H. □

Proof of Proposition 4. Since $\dim S^3 = \dim \mathrm{SO}\,(3) = 3s$ in view of Lemma 2, it suffices to prove only the statement about the kernel. But if $\xi \in \operatorname{Ker}\psi$ then for the quaternion identities i, j, k we have $\xi i = i\xi$, $\xi j = j\xi$ and $\xi k = k\xi$, which is easily seen to be possible only for $\xi \in \mathbb{R}$, i.e. for $\xi = \pm 1$. □

Proposition 4 implies that the mapping $\psi\colon S^3 \to \mathrm{SO}\,(3)$ is a group double covering. Since the sphere S^3 is simply connected, that covering is universal. Therefore $\pi_1 \mathrm{SO}\,(3) =$

$\mathbb{Z}_2$ and hence, by the remarks above, the group $\pi_1 SO(n)$ with any $n \geqslant 3$ is a factor group of the group $\mathbb{Z}_2$. But we know that $\mathbb{Z}_2$ is nontrivial. Therefore, *with* $n \geqslant 3$, *the group* $\pi_1 SO(n)$ *is the second-order group* $\mathbb{Z}_2$.

When $n = 2$ the Lie group SO (2) is a circle S^1 and therefore the *group* $\pi_1 SO(2)$ *is isomorphic to* $\mathbb{Z}$.

When $n = 1$ the group SO (1) is a unit group.

Moreover, we now see that $\mathrm{Spin}_\varepsilon(n)$ *with* $n \geqslant 3$ *is a simply connected group while the covering* φ_0: $\mathrm{Spin}_\varepsilon(n) \to SO(n)$ *is a universal covering.*

In view of the uniqueness of a universal covering it follows, in particular, that $\mathrm{Spin}_+(n)$ *is isomorphic to* Spin (n).

Thus, although $\mathrm{Cl}_+(n)$ and $\mathrm{Cl}(n)$ are not isomorphic, their subgroups $\mathrm{Spin}_+(n)$ and Spin (n) are.

Remark 2. Of course, it is desirable to have the isomorphism between $\mathrm{Spin}_+(n)$ and Spin (n) in a more explicit form. One would also like to understand the algebraic reasons for this isomorphism. Both desires will be satisfied if we construct an isomorphism of $\mathrm{Cl}_+^0(n)$ and $\mathrm{Cl}^0(n)$ mapping $\mathrm{Spin}_+(n)$ onto Spin (n). It turns out that such an isomorphism is the linear isomorphism ρ: $\mathrm{Cl}_+^0(n) \to \mathrm{Cl}^0(n)$ sending the basis element e_I of $\mathrm{Cl}_+^0(n)$ to the basis element $\bar{e}_I$ of $\mathrm{Cl}^0(n)$, i.e. to $(-1)^p e_I$, where $2p = |I|$. Indeed, it obviously suffices to show that ρ is a homomorphism of algebras, i.e. that $\rho(e_I e_J) = \rho(e_I)\rho(e_J)$ for any basis elements e_I, e_J of $\mathrm{Cl}_+^0(n)$. Let $|I| = 2p$, $|J| = 2q$ and $|I \Delta J| = 2r$. Also let τ_+ be the number of pairs $(i, j) \in I \times J$ for which $i > j$ and let τ be the numbers of pairs $(i, j) \in I \times J$ for which $i \geqslant j$. By formulas (12) and (13) $e_I e_J = (-1)^{\tau_+} e_{I\Delta J}$ in $\mathrm{Cl}_+^0(n)$ and $e_I e_J = (-1)^{\tau} e_{I\Delta J}$ in $\mathrm{Cl}^0(n)$. Therefore $\rho(e_I e_J) = (-1)^{\tau_+ + s} e_{I\Delta J}$ and $\rho(e_I)\rho(e_J) = (-1)^{\tau + p + q} e_{I\Delta J}$. This proves all that was to be proved since it is easy to see that $\tau - \tau_+ = |I \cap J| = p + q - s$. □

Remark 3. The fact that the mapping ρ is a homomorphism of algebras can be proved without any calculations if we notice that ρ is a restriction of an isomorphism of complexified algebras $\mathrm{Cl}_+(n) \otimes \mathbb{C}$ and $\mathrm{Cl}(n) \otimes \mathbb{C}$ generated by the correspondences $e_1 \mapsto ie_1, \ldots, e_n \mapsto ie_n$, where $i = \sqrt{-1}$ is an imaginary unit.

As a rule, in what follows we shall consider only the group Spin (n).

Groups Spin (n) with small n are easy to describe.

Clearly, Spin (1) like SO(1) consists of only the unity identity element.

The algebra $\mathbb{C}l^0(2)$ is two-dimensional (its basis consists of elements 1 and e_1e_2) and Spin (2) is a circle in that two-dimensional vector space. Thus

$$\mathrm{Spin}\,(2) \approx SO(2) \approx S^1 \approx U\,(1).$$

As for Spin (3), by virtue of the uniqueness of the universal covering it is isomorphic to the group S^3:

$$\mathrm{Spin}\,(3) \approx S^3 \approx Sp\,(1).$$

It is interesting that the *group* Spin (3) $\approx S^3$ *should be isomorphic to the group* SU(2) *as well.* Indeed, a direct calculation shows that any matrix in SU(2) is of the form

(14) $$\begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix}, \quad \text{where } |a|^2+|b|^2=1$$

and that the mapping $SU(2) \to S^3$ associating matrix (14) with a quaternion $\xi = a + bj \in S^3$ is an isomorphism. □

In particular, it follows that SU(2) *doubly covers the rotation group* SO(3).

To obtain an explicit description of the covering $SU(2) \to SO(3)$ we associate every matrix (14) with a linear fractional transformation

(15) $$z \mapsto \frac{az+b}{-\bar{b}z+\bar{a}}$$

of the augmented plane $\mathbb{C}^+$ of a complex variable. When identifying by stereographic projection of the plane $\mathbb{C}^+$ with the sphere S^2 transformations (15) turn, as is known (see I, 28), into rotations of a sphere, i.e. into SO(3). It is this that gives the covering $SU(2) \to SU(3)$ since matrices differing in sign generate the same rotation (15).

Further, it is easily seen that the *group* Spin (4) *is isomorphic to the direct product* $S^3 \times S^3$ *of groups* $S^3 \approx$ Spin (3). This is most easily established if we notice first that for any two quaternions $\xi, \eta \in S^3$ the formula

$$\zeta \mapsto \xi\zeta\eta, \quad \zeta \in \mathbb{H}$$

defines an isometric (for $|\xi\zeta\bar{\eta}| = |\xi|\cdot|\zeta|\cdot|\bar{\eta}| = |\zeta|$ mapping of the algebra $\mathbb{H}$ into itself, secondly, that the resulting mapping $\mathcal{S}^3 \times \mathcal{S}^3 \to SO(4)$ is a homomorphism (since $\xi_1(\xi_2\zeta\bar{\eta}_2)\bar{\eta}_1 = (\xi_1\xi_2)\zeta(\overline{\eta_1\eta_2})$) and, thirdly, that the kernel of that homomorphism consists of only two elements $(1, 1)$ and $(-1, -1)$ (if $\xi\zeta\bar{\eta} = \zeta$ for all ζ then, in particular $\xi\bar{\eta} = 1$ and hence $\xi = \eta$; consequently $\xi\zeta = \zeta\xi$, from which, as we now know, it follows that $\xi = \pm 1$). This means (see Lemma 1) that the group $\mathcal{S}^3 \times \mathcal{S}^3$ doubly covers SO(4). Hence the covering is universal and therefore $\mathcal{S}^3 \times \mathcal{S}^3$ is isomorphic to Spin (4). □

It turns out that similar results are obtained for the groups Spin (5) and Spin (6). To get them we start with the group SL(4; $\mathbb{C}$) of unimodular linear operators of the complex four-dimensional space $\mathbb{C}^4$. Every operator $A \in SL(4; \mathbb{C})$ obviously induces some linear operator $\widehat{A}\colon \Lambda^2(\mathbb{C}^4) \to \Lambda^2(\mathbb{C}^4)$ in a vector space $\Lambda^2(\mathbb{C}^4)$ of bilinear skew-symmetric functionals in $\mathbb{C}^4$ of (0, 2) type. On bivectors, the operator acts by the formula

$$\widehat{A}(x \wedge y) = Ax \wedge Ay, \qquad x, y \in \mathbb{C}^4.$$

Since $\dim \Lambda^2(\mathbb{C}^4) = 6$, on choosing in the space $\Lambda^2(\mathbb{C}^4)$ a basis consisting of bivectors $e_i \wedge e_j$, $i < j$, where e_1, e_2, e_3, e_4 are vectors of the standard basis of $\mathbb{C}^4$, we may assume $\hat{A}$ to be an element of GL (6; $\mathbb{C}$). Moreover, on considering in $\Lambda^2(\mathbb{C}^4)$ space a quadratic functional Q associating every vector $p^{ij}e_i \wedge e_j$ of $\Lambda^2(\mathbb{C}^4)$ with a number $p^{12}p^{34} + p^{23}p^{14} + p^{13}p^{42}$, we discover from calculation that $\widehat{A}$ preserves the functional Q. (This can be proved geometrically without any calculations as well. Indeed, the operator $\widehat{A}$ sends bivectors to bivectors and therefore preserves the equation $Q = 0$ that is equivalent to the Plucker relation characterizing bivectors among all functionals in $\Lambda^2(\mathbb{C}^4)$; see II, 10, This means that the operator $\widehat{A}$ leaves a second-degree hypersurface $Q = 0$ invariant. But then by the theorem on the uniqueness (up to proportionality) of the equations of second-degree hypersurfaces, the operator $\widehat{A}$ must send the functional Q to a proportional functional

$\lambda_A Q$. Therefore it is only necessary to prove that $\lambda_A = 1$ for any operator $A \in \mathrm{SL}(4, \mathbb{C})$. But the correspondence $A \mapsto \lambda_A$ is obviously a homomorphism of $\mathrm{SL}(4; \mathbb{C})$ into a multiplicative group $\mathbb{C}^*$ of nonzero complex numbers and any such homomorphism can be easily shown to be trivial.)

If we go over from the basis $e_i \wedge e_j$, $i < j$, to a basis

$$
\begin{aligned}
&f_1 = e_1 \wedge e_2 + e_3 \wedge e_4, && f_2 = ie_1 \wedge e_2 - ie_3 \wedge e_4,\\
(16)\quad &f_3 = e_2 \wedge e_3 + e_1 \wedge e_4, && f_4 = ie_2 \wedge e_3 - ie_1 \wedge e_4,\\
&f_5 = e_1 \wedge e_3 + e_4 \wedge e_2, && f_6 = ie_1 \wedge e_3 - ie_4 \wedge e_2,
\end{aligned}
$$

in which Q is written as a sum of squares. then in this basis every operator A will be expressed by an orthogonal matrix. On denoting that matrix by $\chi(A)$ we thus obtain some (obviously homomorphous) mapping

$$\chi\colon \mathrm{SL}(4; \mathbb{C}) \to \mathrm{O}(6; \mathbb{C}).$$

The kernel of the homomorphism χ consists of matrices A whose columns a_1, a_2, a_3, a_4 satisfy the relation $a_i \wedge a_j = e_i \wedge e_j$ for any i, j and so have the property that for every pair (i, j) vectors a_i and a_j can be linearly expressed in terms of vectors e_i and e_j, which is obviously possible only when $a_i = \lambda_i e_i$ for every i. Besides, for any i and j the equation $\lambda_i\lambda_j = 1$ must hold, which is possible only when either $\lambda_i = 1$ or $\lambda_i = -1$ for every i. This proves that the second-order group $\{E, -E\}$ is the kernel of χ.

Consider now in $\mathrm{SL}(4; \mathbb{C})$ a subgroup consisting of matrices A for which a matrix $\chi(A)$ has real coefficients, i.e. it is in the group $\mathrm{O}(6) = \mathrm{O}(6, \mathbb{R})$. Clearly, A is in that group if and only if the operator $\widehat{A}$ is commutative with a semilinear transformation $S\colon \bigwedge^2 (\mathbb{C}^4) \to \bigwedge^2 (\mathbb{C}^4)$ replacing all the coordinates of every element of the vector space $\bigwedge^2 (\mathbb{C}^4)$ relative to basis (16) by complex conjugate numbers. If the functional from the space $\bigwedge^2 (\mathbb{C}^4)$ has the coordinates $z_1, \ldots, z_6$ in the basis (16), then in the basis consisting of bivectors $e_i \wedge e_j$, $i < j$, it has coordinates

$$
\begin{aligned}
p_{12} &= z_1 + iz_2, & p_{34} &= z_1 - iz_2,\\
p_{23} &= z_3 + iz_4, & p_{14} &= z_3 - iz_4,\\
p_{13} &= z_5 + iz_6, & p_{24} &= -z_5 + iz_6,
\end{aligned}
$$

and therefore the transformation S sends it to a functional with coordinates

$$\bar{p}_{34}, \quad \bar{p}_{12}, \quad \bar{p}_{14}, \quad \bar{p}_{23}, \quad -\bar{p}_{24}, \quad -\bar{p}_{13}.$$

This means that $S = T \circ \widehat{\sigma}$, where T is a linear operator $\Lambda^2(\mathbb{C}^4) \to \Lambda^2(\mathbb{C}^4)$ acting in basis bivectors by the formulas

$$(17)\quad \begin{aligned} T(e_1 \wedge e_2) &= e_3 \wedge e_4, & T(e_3 \wedge e_4) &= e_1 \wedge e_2, \\ T(e_2 \wedge e_3) &= e_1 \wedge e_4, & T(e_1 \wedge e_4) &= e_2 \wedge e_3, \\ T(e_1 \wedge e_3) &= -e_2 \wedge e_4, & T(e_2 \wedge e_4) &= -e_1 \wedge e_3, \end{aligned}$$

and $\sigma: \mathbb{C}^4 \to \mathbb{C}^4$ is a semilinear isomorphism replacing the components of every vector by complex conjugate numbers. Thus $\chi(A) \in O(6)$ if and only if

$$\widehat{A} \circ T \circ \widehat{\sigma} = T \circ \widehat{\sigma} \circ \widehat{A}.$$

We shall show below that for any operator $A \in SL(4; \mathbb{C})$

$$(18)\qquad \widehat{A} \circ T = T \circ \widehat{A^c},$$

where A^c is an operator on $\mathbb{C}^4$ whose matrix is obtained from the matrix of A by transposition and passage to the inverse matrix. It follows that $\chi(A) \in O(6)$ if and only if $\widehat{A^c} \circ \widehat{\sigma} = \widehat{\sigma} \circ \widehat{A}$, i.e. if $\widehat{A^c \circ \sigma} = \widehat{\sigma \circ A}$. In particular, $\chi(A) \in O(6)$ if $A^c \circ \sigma = \sigma \circ A$, i.e. if $A^* = A^{-1}$, where A^* is the conjugate (relative to the standard scalar multiplication in $\mathbb{C}^4$) operator (whose matrix is obtained from the matrix of A by transposition and complex conjugation). Since the equation $A^* = A^{-1}$ characterizes unitary operators in the subgroup $SU(4)$ of $SL(4; \mathbb{C})$, this proves that the homomorphism χ maps the group $SU(4)$ into $O(6)$ and hence, $SU(4)$ being a connected group, into $SO(6)$. It therefore induces a homomorphism

$$\chi_0: SU(4) \to SO(6).$$

Since the kernel of χ_0 coincides with that of χ and is therefore a second-order group and $\dim SU(4) = \dim SO(6) = 15$, the homomorphism χ_0 is a double covering. This proves that the *group* $SU(4)$ *doubly covers* $SO(6)$ *and is therefore isomorphic to* Spin (6).

The group SU(4) contains a subgroup Sp(2) whose elements A are characterized by the property that they leave invariant a skew-symmetric bilinear functional with matrix

$$J=\begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 0 \\ -1 & 0 & 0 & 0 \end{pmatrix},$$

or equivalently by the property that $A^cJ = JA$, where J is a linear operator on $\mathbb{C}^4$ with matrix J (cf. formula (5) of Lecture 1). Therefore if $A \in \mathrm{Sp}(2)$, then $\hat{A}^c \circ \hat{J} = \widehat{J} \circ \widehat{A}$ and hence (see formula (18)) $\widehat{A} \circ T \circ \widehat{J} = T \circ \widehat{J} \circ \widehat{A}$. Calculation shows that $T \circ \widehat{J} = -I$, where I is a linear operator $\Lambda^2(\mathbb{C}^4) \to \Lambda^2(\mathbb{C}^4)$ leaving all vectors (16) fixed, except vector f_3 which goes into vector $-f_3$. Thus $\widehat{A} \circ I = I \circ \widehat{A}$, which is equivalent to $\hat{A}f_3 = \pm f_3$. This means that $\chi(A)$ is contained in a subgroup of SO(6) isomorphic to SO(5) and even, in view of the connectedness of Sp(2), in the component of the identity SO(5) of that subgroup. Since $\dim \mathrm{Sp}(2) = \dim \mathrm{SO}(5) = 10$, this proves that the *group* Sp(2) *doubly covers* SO(5) *and is therefore isomorphic to* Spin (5).

Collecting all the proved facts together we obtain the following proposition:

Proposition 6. *Groups*

$$S^1,\quad S^3 = \mathrm{Sp}(1) = \mathrm{SU}(2),\quad S^3 \times S^3,\quad \mathrm{Sp}(2),\quad \mathrm{SU}(4)$$

doubly cover the groups

$$\mathrm{SO}(2),\quad \mathrm{SO}(3),\quad \mathrm{SO}(4),\quad \mathrm{SO}(5),\quad \mathrm{SO}(6)$$

and are therefore isomorphic to the groups

$$\mathrm{Spin}\,(2),\quad \mathrm{Spin}\,(3),\quad \mathrm{Spin}\,(4),\quad \mathrm{Spin}\,(5),\quad \mathrm{Spin}\,(6)$$

respectively. □

Thus we have succeeded in representing groups Spin (6) with $n \leqslant 6$ as matrix groups. Similar results hold for $n > 6$, the difference, however, being that groups Spin (n), $n > 6$, are identified only with some subgroups of the corresponding orthogonal groups.

Clearly, to prove that statement it suffices to obtain matrix representations of complete Clifford algebras $\mathrm{Cl}_\varepsilon(n)$. In those representations we shall neglect $\mathbb{Z}_2$-graduation and therefore, in particular, assume all tensor products to be ordinary (not skew).

We now know that $\mathrm{Cl}\,(1) \approx \mathbb{C}$ and $\mathrm{Cl}_+\,(1) \approx \mathbb{D}$ where $\mathbb{D}$ is the algebra of double numbers $a + be$, $e^2 = 1$. It is easy to see, however, that the correspondence $a + be \mapsto (a + b, a - b)$ is an isomorphism $\mathbb{D} \approx \mathbb{R} \oplus \mathbb{R}$. Thus

$$\mathrm{Cl}\,(1) \approx \mathbb{C}, \qquad \mathrm{Cl}_+\,(1) \approx \mathbb{R} \oplus \mathbb{R}.$$

Further, a check shows that correspondences $e_1 \mapsto i$, $e_2 \mapsto j$, $e_1e_2 \mapsto k$ define an isomorphism of the algebra $\mathrm{Cl}\,(2)$ with an algebra of quaternions $\mathbb{H}$ and correspondences

$$e_1 \mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad e_2 \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad e_1e_2 \mapsto \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

do an isomorphism $\mathrm{Cl}_+\,(2) \approx \mathbb{R}\,(2)$. Thus

$$\mathrm{Cl}\,(2) \approx \mathbb{H}, \qquad \mathrm{Cl}_+\,(2) \approx \mathbb{R}\,(2).$$

Proposition 7. *For any $n \geqslant 0$ there is an isomorphism*

$$\mathrm{Cl}_\varepsilon\,(n + 2) \approx \mathrm{Cl}_{-\varepsilon}\,(n) \otimes \mathrm{Cl}_\varepsilon\,(2),$$

i.e. two isomorphisms

$$\mathrm{Cl}\,(n + 2) \approx \mathrm{Cl}_+\,(n) \otimes \mathbb{H},$$

$$\mathrm{Cl}_+\,(n + 2) \approx \mathrm{Cl}\,(n) \otimes \mathbb{R}\,(2).$$

Proof. Consider a linear mapping

$$\alpha\colon \mathbb{R}^{n+2} \to \mathrm{Cl}_{-\varepsilon}\,(n) \otimes \mathrm{Cl}_\varepsilon\,(2)$$

for which

$$\alpha\,(e_i) = e_i \otimes e_1e_2 \quad \text{for } i = 1, \ldots, n,$$

$$\alpha\,(e_{n+1}) = 1 \otimes e_1, \qquad \alpha\,(e_{n+2}) = 1 \otimes e_2$$

(we denote by the same symbols e_i the generators of all the three algebras $\mathrm{Cl}_\varepsilon\,(n + 2)$, $\mathrm{Cl}_{-\varepsilon}\,(n)$ and $\mathrm{Cl}_\varepsilon\,(2)$). A check shows that $\alpha\,(x)^2 = \varepsilon\,|\,x\,|^2$ for any $x \in \mathbb{R}^{n+2}$. Therefore the mapping α can be extended to some homomorphism $\alpha^\#\colon \mathrm{Cl}_\varepsilon\,(n + 2) \to \mathrm{Cl}_{-\varepsilon}\,(n) \otimes \mathrm{Cl}_\varepsilon\,(2)$ of $\mathrm{Cl}_\varepsilon\,(n + 2)$ into an algebra $\mathrm{Cl}_{-\varepsilon}\,(n) \otimes \mathrm{Cl}_\varepsilon\,(2)$. A similar

reasoning yields homomorphisms $\beta^{\#}\colon \mathbb{C}\mathrm{l}_{-\varepsilon}(n) \to \mathbb{C}\mathrm{l}_{\varepsilon}(n+2)$ and $\gamma^{\#}\colon \mathbb{C}\mathrm{l}_{\varepsilon}(2) \to \mathbb{C}\mathrm{l}_{\varepsilon}(n+2)$ for which

$$\beta^{\#}(e_i) = -e_i e_{n+1} e_{n+2}, \qquad i = 1, \ldots, n,$$

and

$$\gamma^{\#}(e_1) = e_{n+1}, \qquad \gamma^{\#}(e_2) = e_{n+2}.$$

Since, as is easily seen, $\beta^{\#}(e_i)\gamma^{\#}(e_j) = \gamma^{\#}(e_j)\beta^{\#}(e_i)$ for any $i = 1, \ldots, n$, and $j = 1, 2$, the homomorphisms $\beta^{\#}$ and $\gamma^{\#}$ commute and hence the mapping

$$\beta^{\#} \otimes \gamma^{\#}\colon \mathbb{C}\mathrm{l}_{-\varepsilon}(n) \otimes \mathbb{C}\mathrm{l}_{\varepsilon}(2) \to \mathbb{C}\mathrm{l}_{\varepsilon}(n+2)$$

is a homomorphism of algebras. For every $i = 1, \ldots, n$ we have

$$[(\beta^{\#} \otimes \gamma^{\#}) \circ \alpha^{\#}](e_i) = \beta^{\#}(e_i)\cdot\gamma^{\#}(e_1e_2) = -e_i(e_{n+1}e_{n+2})^2 = e_i$$

(since $(e_1, e_2)^2 = -1$ for any ε) and for every $j = 1, 2$ we have

$$[(\beta^{\#} \otimes \gamma^{\#}) \circ \alpha^{\#}](e_{n+j}) = 1 \otimes \gamma^{\#}(e_j) = 1 \otimes e_{n+j},$$

so that $(\beta^{\#} \otimes \gamma^{\#}) \circ \alpha^{\#} = \mathrm{id}$. Similarly, for any $i = 1, \ldots, n$

$$\begin{aligned}[][\alpha^{\#} \circ (\beta^{\#} \otimes \gamma^{\#})](e_i \otimes 1) = \alpha^{\#}(\beta^{\#}(e_i)) &= \alpha^{\#}(-e_i e_{n+1} e_{n+2}) \\ &= -\alpha^{\#}(e_i)\,\alpha^{\#}(e_{n+1})\,\alpha^{\#}(e_{n+2}) \\ &= -(e_i \otimes e_1e_2)(1 \otimes e_1)(1 \otimes e_2) \\ &= -e_i \otimes (e_1e_2)^2 = e_i\end{aligned}$$

and for any $j = 1, 2$

$$\begin{aligned}[][\alpha^{\#} \circ (\beta^{\#} \otimes \gamma^{\#})](1 \otimes e_j) &= \alpha^{\#}(\gamma^{\#}(e_j)) \\ &= \alpha^{\#}(e_{n+j}) = 1 \otimes e_j,\end{aligned}$$

from which it follows immediately that $\alpha^{\#} \circ (\beta^{\#} \otimes \gamma^{\#}) = \mathrm{id}$. Thus the mappings $\alpha^{\#}$ and $\beta^{\#} \otimes \gamma^{\#}$ are reciprocal isomorphisms. $\square$

It follows immediately from this proposition that

$$\mathbb{C}\mathrm{l}(3) \approx (\mathbb{R} \oplus \mathbb{R}) \otimes \mathbb{H} \approx \mathbb{H} \oplus \mathbb{H},\ \mathbb{C}\mathrm{l}_{+}(3) \approx \mathbb{C} \otimes \mathbb{R}(2) \approx \mathbb{C}(2),$$

$$\mathbb{C}\mathrm{l}(4) \approx \mathbb{R}(2) \otimes \mathbb{H} \approx \mathbb{H}(2),\ \mathbb{C}\mathrm{l}_{+}(4) \approx \mathbb{H} \otimes \mathbb{R}(2) \approx \mathbb{H}(2).$$

To proceed we need the following lemma:

Lemma 3. *There are isomorphisms*

$$\mathbb{C} \otimes \mathbb{C} \approx \mathbb{C} \oplus \mathbb{C}, \quad \mathbb{C} \otimes \mathbb{H} \approx \mathbb{C}\,(2), \quad \mathbb{H} \otimes \mathbb{H} \approx \mathbb{R}\,(4).$$

Proof. Clearly, $\mathbb{C} \otimes \mathrm{Cl}\,(n) \approx \mathbb{C} \otimes \mathrm{Cl}_+\,(n)$. Therefore

$$\mathbb{C} \otimes \mathbb{C} + \mathbb{C} \otimes \mathrm{Cl}\,(1) \approx \mathbb{C} \otimes \mathrm{Cl}_+\,(1) \approx \mathbb{C} \otimes (\mathbb{R} \oplus \mathbb{R}) \approx \mathbb{C} \oplus \mathbb{C}.$$

Similarly

$$\mathbb{C} \otimes \mathbb{H} \approx \mathbb{C} \otimes \mathrm{C}\,(2) \approx \mathbb{C} \otimes \mathrm{C}_+\,(2) \approx \mathbb{C} \otimes \mathbb{R}\,(2) \approx \mathbb{C}\,(2).$$

However, these isomorphisms are easy to establish directly as well. For example, the isomorphism $\mathbb{C} \otimes \mathbb{C} \approx \mathbb{C} \oplus \mathbb{C}$ is defined by the correspondences $1 \otimes 1 \mapsto (1, 1)$, $i \otimes 1 \mapsto (i, i)$, $1 \otimes i \mapsto (i, -i)$, $i \otimes i \mapsto (-1, 1)$.

The isomorphism $\mathbb{H} \otimes \mathbb{H} \approx \mathbb{R}\,(4)$ is established if we identify $\mathbb{H}$ with $\mathbb{R}^4$ and associate any element of $\mathbb{H} \otimes \mathbb{H}$ of the form $\xi \otimes \eta$, where $\xi, \eta \in \mathbb{H}$ with a linear operator $\omega\,(\xi \otimes \eta)\colon \mathbb{H} \to \mathbb{H}$ acting by the formula

$$\omega\,(\xi \otimes \eta)\,\zeta = \xi\zeta\bar{\eta}, \qquad \zeta \in \mathbb{H}.$$

A check shows that the operator $\omega\,(\xi \otimes \eta)$ is correctly defined (i.e. if $\xi \otimes \eta = \xi' \otimes \eta'$, then $\omega\,(\xi \otimes \eta) = \omega\,(\xi' \otimes \eta')$) and that by linearity the mapping ω can be correctly extended to some homomorphism ω of the algebra $\mathbb{H} \otimes \mathbb{H}$ into the algebra of linear operators $\mathbb{H} \to \mathbb{H}$, i.e. in view of the identification of $\mathbb{H}$ with $\mathbb{R}^4$, into the algebra of matrices $\mathbb{R}\,(4)$. Since $i1\bar{i} = 1$, $ii\bar{i} = i$, $ij\bar{i} = -j$, $ik\bar{i} = -k$, we have

$$\omega\,(i \otimes i) = E_{11} + E_{22} - E_{33} - E_{44},$$

and since $i1\bar{j} = -k$, $ii\bar{j} = j$, $ij\bar{j} = i$, $ik\bar{j} = -1$, we have

$$\omega\,(i \otimes j) = -E_{14} + E_{23} + E_{32} - E_{41}.$$

In a similar fashion we can calculate all the sixteen matrices $\omega(\xi \otimes \eta)$, where $\xi, \eta = 1, i, j, k$ (of course, $\omega\,(1 \otimes 1)$ is the unit matrix $E = E_{11} + E_{22} + E_{33} + E_{44}$). On making these calculations we at once discover that any matrix unit $E_{\alpha\beta}$, $1 \leqslant \alpha, \beta \leqslant 4$, can be represented as a linear

combination of matrices $\omega(\xi \otimes \eta)$. For example,

$$E_{11} = \frac{1}{4}\omega(1 \otimes 1 + i \otimes i + j \otimes j + k \otimes k)$$

and

$$E_{12} = \frac{1}{4}\omega(i \otimes 1 - 1 \otimes i + k \otimes j - j \otimes k).$$

Hence the mapping ω is an epimorphism and therefore, in view of the equality of the dimensions of the algebras $\mathbb{H} \otimes \mathbb{H}$ and $\mathbb{R}(4)$, an isomorphism as well. $\square$

Given an algebra $\mathcal{A}$ we shall denote by $\mathcal{A}(n)$ an algebra of square $n \times n$ matrices over $\mathcal{A}$, i.e. with elements in $\mathcal{A}$. If $E_{\alpha\beta}$ are as ever matrix units, then the correspondence $a \otimes E_{\alpha\beta} \mapsto aE_{\alpha\beta}$ is easily seen to extend to an isomorphism

$$\mathcal{A} \otimes \mathbb{R}(n) \approx \mathcal{A}(n).$$

Since an algebra $\mathbb{R}(n)(m)$ of $m \times m$ matrices whose elements are $n \times n$ matrices can be naturally identified with an algebra $\mathbb{R}(mn)$ of order mn, it follows in particular that

$$\mathbb{R}(m) \otimes \mathbb{R}(n) \approx \mathbb{R}(mn)$$

for any numbers $m, n \geqslant 0$. Therefore

$$\begin{aligned}\mathcal{A}(m) \otimes \mathcal{B}(n) &\approx (\mathcal{A} \otimes \mathbb{R}(m)) \otimes (\mathcal{B} \otimes \mathbb{R}(n)) \\ &\approx (\mathcal{A} \otimes \mathcal{B}) \otimes (\mathbb{R}(m) \otimes \mathbb{R}(n)) \approx (\mathcal{A} \otimes \mathcal{B})(mn)\end{aligned}$$

for any algebras $\mathcal{A}$, $\mathcal{B}$ and any numbers $m, n \geqslant 0$.

Hence by Lemma 3

$$\mathbb{C}(m) \otimes \mathbb{H}(n) \approx \mathbb{C}(2mn), \qquad \mathbb{H}(m) \otimes \mathbb{H}(n) \approx \mathbb{R}(4mn).$$

Returning to Clifford algebras we in the first place get

$$\mathrm{Cl}_+(2) \otimes \mathrm{Cl}(2) \approx \mathbb{H} \otimes \mathbb{R}(2) \approx \mathbb{H}(2).$$

By applying Proposition 7 twice we therefore obtain the isomorphisms

$$\mathrm{Cl}(n+4) \approx \mathrm{Cl}(n) \otimes \mathbb{H}(2) \text{ and } \mathrm{Cl}_+(n+4) \approx \mathrm{Cl}_+(n) \otimes \mathbb{H}(2)$$

from which, in view of the isomorphism $\mathbb{H}(2) \otimes \mathbb{H}(2) \approx \mathbb{R}(16)$, it then follows that

$$\mathrm{Cl}(n+8) \approx \mathrm{Cl}(n) \otimes \mathbb{R}(16) \approx \mathrm{Cl}(n)(16)$$

and

$$\mathrm{Cl}_+(n+8) \approx \mathrm{Cl}_+(n) \otimes \mathbb{R}(16) \approx \mathrm{Cl}_+(n)(16).$$

Since we have already calculated algebras $\mathrm{Cl}_\varepsilon(n)$ with $n \leqslant 4$, this yields algebras $\mathrm{Cl}_\varepsilon(n)$ for all n. We shall state the final result as the following theorem:

Theorem 2. *There are isomorphisms*

$$\begin{array}{ll}
\mathrm{Cl}(8m-3) \approx \mathbb{C}(2^{4m-2}), & \mathrm{Cl}_+(8m-3) \approx \mathbb{H}(2^{4m-3}) \oplus \mathbb{H}(2^{4m-3}), \\
\mathrm{Cl}(8m-2) \approx \mathbb{R}(2^{4m-1}), & \mathrm{Cl}_+(8m-2) \approx \mathbb{H}(2^{4m-2}), \\
\mathrm{Cl}(8m-1) \approx \mathbb{R}(2^{4m-1}) \oplus \mathbb{R}(2^{4m-1}) & \mathrm{Cl}_+(8m-1) \approx \mathbb{C}(2^{4m-1}), \\
\mathrm{Cl}(8m) \approx \mathbb{R}(2^{4m}), & \mathrm{Cl}_+(8m) \approx \mathbb{R}(2^{4m}), \\
\mathrm{Cl}(8m+1) \approx \mathbb{C}(2^{4m}), & \mathrm{Cl}_+(8m+1) \approx \mathbb{R}(2^{4m}) \oplus \mathbb{R}(2^{4m}), \\
\mathrm{Cl}(8m+2) \approx \mathbb{H}(2^{4m}), & \mathrm{Cl}_+(8m+2) \approx \mathbb{R}(2^{4m+1}), \\
\mathrm{Cl}(8m+3) \approx \mathbb{H}(2^{4m}) \oplus \mathbb{H}(2^{4m}), & \mathrm{Cl}_+(8m+3) \approx \mathbb{C}(2^{4m+1}), \\
\mathrm{Cl}(8m+4) \approx \mathbb{H}(2^{4m+1}), & \mathrm{Cl}_+(8m+4) \approx \mathbb{H}(2^{4m+1}). \ \square
\end{array}$$

Notice that

$$\mathrm{Cl}(8m) \approx \mathrm{Cl}_+(8m), \qquad \mathrm{Cl}(8m+4) \approx \mathrm{Cl}_+(8m+4).$$

No other algebras $\mathrm{Cl}(n)$ and $\mathrm{Cl}_+(n)$ are isomorphic to each other. It is also useful to keep in mind that

$$\mathbb{R}(2^n) = \begin{cases} \mathrm{Cl}(2n) & \text{if } n = 4m-1,\ 4m, \\ \mathrm{Cl}_+(2n) & \text{if } n = 4m+1, \end{cases}$$

and similarly for $\mathbb{C}(2^n)$ and $\mathbb{H}(2^n)$. It is interesting that the algebra $\mathbb{R}(^{4m+2})$ should not be isomorphic to any algebra $\mathrm{Cl}_\varepsilon(n)$.

It follows for groups $\mathrm{Spin}(n)$ (and $\mathrm{pin}_\varepsilon(n)$) from Theorem 2 that they are embedded into the corresponding matrix

groups or their direct sums. But since any pair (A, B) of $n \times n$ matrices are identified with the $2n \times 2n$ matrix

$$\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix} \tag{19}$$

embedding into direct sums can be replaced by embeddings into groups of matrices twice their size. Thus *elements of groups* Spin (n) *can be represented by matrices of some order* N *over algebras* $\mathbb{R}$, $\mathbb{C}$ *or* $\mathbb{H}$, *with* N *being equal to* $2^{\alpha(n)}$, *where*

$$\alpha(n) = \begin{cases} 4m-2 & \text{if} \quad n = 8m-3, \\ 4m-1 & \text{if} \quad n = 8m-2, \\ 4m & \text{if} \quad n = 8m-1,\ 8m,\ 8m+1,\ 8m+2, \\ 4m+1 & \text{if} \quad n = 8m+3,\ 8m+4, \end{cases}$$

and the matrices being real at $n = 8m-2,\ 8m-1,\ 8m$, *complex at* $n = 8m-3,\ 8m+1$ *and quaternion ones at* $n = 8m+2,\ 8m+3,\ 8m+4$.

However, when a pair (A, B) is identified with matrix (19) there is a certain loss of information. So it is more appropriate not to make the identification but represent elements of groups Spin (n) with $n = 8m-1$ and $n = 8m+3$ by pairs of matrices of order $2^{\alpha(n)-1}$ (real or quaternion ones respectively).

Definition 5. Two matrix representations of a group G, i.e. two embeddings (or more generally two homomorphisms) of G into some matrix group are said to be *equivalent* if they differ by an internal automorphism of that group, i.e. if they are obtained from the same representation of G as a group of linear operators of some vector space by a different choice of basis in that vector space.

It is important to bear in mind that the *above representations of groups* Spin (n) *are defined up to an equivalence only*, since isomorphisms in Proposition 7 and Lemma 2 can be constructed in many ways having no advantages over one another (it may be assumed, for example, that $\alpha(e_1) = 1 \otimes e_1$, $\alpha(e_2) = 1 \otimes e_2$ and $\alpha(e_i) = e_{i-2} \otimes e_1 e_2$ for $2 \leqslant i \leqslant n+2$).

It is interesting that this statement can be made more precise.

Let us say that the matrix (over a unital algebra $\mathscr{A}$) is *monomial* if all elements in each row and each column are zero, except one which is ± 1. The operator corresponding to the monomial matrix interchanges basis vectors multiplying them at the same time by ± 1. Therefore any monomial matrix is an orthogonal one when $\mathscr{A} = \mathbb{R}$, a unitary one when $\mathscr{A} = \mathbb{C}$ and a symplectic one when $\mathscr{A} = \mathbb{H}$.

The arbitrariness in the isomorphisms of Proposition 7 and Lemma 2 can obviously be restricted to interchanges of basis elements which would be accompanied by multiplication of the latter by ± 1. Therefore the *constructed representations of groups* Spin (n) *may be assumed defined up to equivalences effected by monomial matrices.*

It is clear that for any monomial matrices $A \in \mathbb{R}(m)$ and $B \in \mathbb{R}(n)$ the matrix in $\mathbb{R}(mn) \approx \mathbb{R}(m) \otimes \mathbb{R}(n)$ corresponding to a tensor product $A \otimes B$ (by the way, this matrix is called the *Kronecker product* of A and B) is also monomial.

In addition it is easy to see that under isomorphisms $\mathbb{C} \otimes \mathbb{H} \approx \mathbb{C}(2)$ and $\mathbb{H} \otimes \mathbb{H} \approx \mathbb{R}(4)$ of Lemma 2 the generators $\xi \otimes \eta$, where $\xi = 1, i$ or $\xi = 1, i, j, k$ and $\eta = 1, i, j, k$, turn into monomial matrices. The same property holds for the isomorphisms $\mathrm{Cl}_+(2) \approx \mathbb{R}(2)$ (with respect to the generators e_1 and e_2). Therefore it follows by an induction that *under isomorphisms of Theorem* 2 *the generators* $e_1, \ldots, e_n$ *of algebras* $\mathrm{Cl}(n)$ *turn into monomial matrices* $E_1, \ldots, E_n$ (*or into pairs of monomial matrices*).

In particular, if $E_1, \ldots, E_n$ are real matrices, then they are orthogonal and if $E_1, \ldots, E_n$ are complex or quaternion matrices, then they are respectively unitary or symplectic. In other words, these matrices satisfy the identity $U\bar{U}^\top = E$, where E is the identity matrix. But since $e_i^2 = -1$, we have $E_i^2 = -E$ and therefore $\bar{E}_i^\top = -E_i$. Hence $\bar{U}^\top = -U$ for every matrix U of the form E_i and hence, by linearity, for every matrix U of the form u^iE_i representing an element $u = u^ie_i \in \iota\mathbb{R}^n \subset \mathrm{Cl}(n)$. On the other hand, since $u^2 = -|u|^2$, we have $U^2 = -|u|^2E$ and, in particular, $U^2 = -E$ for $u \in S^{n-1}$. Therefore $U\bar{U}^\top = E$, i.e. U is an orthogonal matrix or it is respectively unitary or symplectic.

Putting for notational simplicity

$$\mathrm{O}_{\mathbb{K}}(n)=\begin{cases}\mathrm{O}(n) & \text{if} \quad \mathbb{K}=\mathbb{R}\\ \mathrm{U}(n) & \text{if} \quad \mathbb{K}=\mathbb{C}\\ \mathrm{Sp}(n) & \text{if} \quad \mathbb{K}=\mathbb{H}\end{cases}$$

we thus find that *every element* $u \in S^{n-1} \subset \mathrm{Cl}(n)$ *can be represented by a matrix* U *in the group* $\mathrm{O}_{\mathbb{K}}(n)$, *where* $\mathbb{K} = \mathbb{R}$, $\mathbb{C}$ or $\mathbb{H}$ *depending on* n.

Since elements in S^{n-1} generate a group pin (n), this conclusion is true for any element $u \in \mathrm{pin}(n)$ too, and, in particular, for any element $u \in \mathrm{Spin}(n)$.

Thus the *group* Spin (n) *turns out to be embedded into* $\mathrm{O}_{\mathbb{K}}(2^{\alpha(n)})$, *where*

$$\mathbb{K}=\begin{cases}\mathbb{R} \text{ for } n=8m-2,\ 8m-1,\ 8m,\\ \mathbb{C} \text{ for } n=8m-3,\ 8m+1,\\ \mathbb{H} \text{ for } n=8m+2,\ 8m+3,\ 8m+4.\end{cases}$$

When $\mathbb{K} = \mathbb{R}$ it is possible to state in addition, in view of the connectedness of the group Spin (n), that $\mathrm{Spin}(n) \subset \mathrm{SO}(n)$.

In the case $\mathbb{K} \neq \mathbb{R}$ it is, of course, possible to go over by identifying $\mathbb{C}$ with $\mathbb{R}^2$ and $\mathbb{H}$ with $\mathbb{R}^4$ to real (necessarily orthogonal and unimodular) matrices; however, this will not only double or quadruple the dimension but also lead to an essential loss of information.

When $n = 8m - 1$ or $n = 8m + 3$ we in fact effect the representation of the elements of a group Spin (n) by pairs of matrices half the order.

Note that we have ignored the possibility of obtaining another series of representations by using the algebra $\mathrm{Cl}_+(n)$ and the isomorphism $\mathrm{Spin}(n) \approx \mathrm{Spin}_+(n)$. The reason for this is that these representations essentially give nothing new leading as they do to equivalent representations or to representations resulting from them by realizing, complexifying or constructing a direct sum.

There is, however, another possibility of constructing representations of groups Spin (n), which while actually giving nothing new helps define more precisely the structure of the representations already constructed.

This possibility is based on the fact that by definition the group Spin (n) is contained in a subalgebra $\mathbb{C}l^0(n)$ of $\mathbb{C}l(n)$ consisting of even elements.

Proposition 8. *For any* $n \geqslant 1$ *an algebra* $\mathbb{C}l^0(n)$ *is isomorphic to* $\mathbb{C}l(n-1)$.

Proof. We define a linear mapping

$$\omega\colon \mathbb{C}l(n-1) \to \mathbb{C}l^0(n),$$

by putting

$$\omega(e_I) = \begin{cases} e_I & \text{if } |I| \text{ is even} \\ e_I e_n & \text{if } |I| \text{ is odd} \end{cases}$$

for any basis element e_I of an algebra $\mathbb{C}l(n-1)$, where I is a subset of the set $[n-1] = \{1, \ldots, n-1\}$. In other words, $\omega(e_I) = e_{I^+}$, where

$$I^+ = \begin{cases} I & \text{if } |I| \text{ is even,} \\ I \cup \{n\} & \text{if } |I| \text{ is odd.} \end{cases}$$

Denoting as before by $\tau(I, J)$ the number of pairs $(i, j) \in I \times J$ for which $i \geqslant j$, we at once get

$$\tau(I^+, J^+) \equiv \tau(I, J) \bmod 2.$$

In addition, it is easy to see that $I^+ \Delta J^+ = (I \Delta J)^+$. Hence (see formula (13))

$$\begin{aligned} \omega(e_I)\,\omega(e_J) &= e_{I^+}e_{J^+} = (-1)^{\tau(I^+, J^+)}\, e_{I^+\Delta J^+} \\ &= (-1)^{\tau(I, J)}\, e_{(I\Delta J)^+} = \omega(e_I e_J) \end{aligned}$$

for any basis elements e_I and e_J of $\mathbb{C}l(n-1)$. Hence ω is a homomorphism of algebras and therefore (effecting as it does a bijective correspondence between their bases) also an isomorphism. $\square$

Note that the inverse isomorphism ω^{-1} acts by the formula

$$\omega^{-1}(u + ve_n) = u + v,$$

where at the left-hand side u and v are elements of an algebra $\mathbb{C}l(n)$ (in $\mathbb{C}l^0(n)$ and $\mathbb{C}l^1(n)$, respectively) that contain no e_n, i.e. that can be decomposed into basis vectors e_I with $I \subset [n-1]$, and at the right-hand side u and v are the "same" elements of $\mathbb{C}l(n-1)$.

Remark 4. As we know, $\mathbb{C}l^0(n)$ and $\mathbb{C}l_+^0(n)$ are isomorphic. Therefore $\mathbb{C}l(n-1)$ *is isomorphic also to* $\mathbb{C}l_+^0(n)$. In explicit form the isomorphism $\omega_+ : \mathbb{C}l(n-1) \to \mathbb{C}l_+^0(n)$ is given by the formulas

$$\omega_+(e_I) = \begin{cases} \bar{e}_I & \text{if } |I| \text{ is even,} \\ e_n \bar{e}_I & \text{if } |I| \text{ is odd.} \end{cases}$$

It may be assumed by Proposition 8 that Spin $(n) \subset \mathbb{C}l(n-1)$. Therefore by applying again Theorem 2 we obtain a *representation of elements of* Spin (n) *by matrices of order* $2^{\alpha(n-1)}$ *over an algebra* $\mathbb{K}$, *where*

$$\mathbb{K} = \begin{cases} \mathbb{R} & \text{if } n = 8m-1,\ 8m,\ 8m+1, \\ \mathbb{C} & \text{if } n = 8m-2,\ 8m+2, \\ \mathbb{H} & \text{if } n = 8m+3,\ 8m+4,\ 8m+5. \end{cases}$$

For $n = 8m$ and $n = 8m + 4$, of course, we in fact obtain a pairwise representation of matrices of order $2^{\alpha(n-1)-1}$.

Any vector $u \in \mathbb{R}^n$ can be written as $u = u' + \lambda e_n$, where $u' \in \mathbb{R}^{n-1}$ and $\lambda \in \mathbb{R}$, with $u \in S^{n-1}$ if and only if $|u'|^2 + \lambda^2 = 1$. By definition a group Spin (n) is generated by all possible elements of the form uv, where $u, v \in S^{n-1}$, i.e. by elements of the form

$$(u' + \lambda e_n)(v' + \mu e_n) = (u'v' - \lambda\mu) + (\mu u' - \lambda v') e_n,$$

and hence its image in $\mathbb{C}l(n-1)$ is generated by elements of the form $(u'v' - \lambda\mu) + (\mu u' - \lambda v')$. But putting $v^* = v' - \mu e_n$ we find that the element

$$ue_n \cdot v^* e_n = (u'e_n - \lambda)(v'e_n + \mu) = (u'v' - \lambda\mu) + (\mu u' - \lambda v') e_n$$

has in $\mathbb{C}l^0(n-1)$ the same image $(u'v' - \lambda\mu) + (\mu u' - \lambda v')$ as an element uv. This shows (since $ue_n \in$ Spin (n) and $v^* \in S^{n-1}$ if $v \in S^{n-1}$) that the image of Spin (n) in $\mathbb{C}l^0(n-1)$ is generated by the images of elements of the form ue_n, $u \in S^{n-1}$. Since $ue_n = u'e_n - \lambda$, these images are of the form $u' - \lambda$ and hence can be represented by

matrices of the form $U - \lambda E$. Since $\bar{U}^{\intercal} = -U$ and hence

$$\begin{aligned}(U - \lambda E)(\bar{U} - \lambda E)^{\intercal} &= -(U - \lambda E)(U + \lambda E) \\ &= -U^2 + \lambda^2 E = (|u'|^2 + \lambda^2) E \\ &= E,\end{aligned}$$

all these matrices are orthogonal (or unitary or symplectic, respectively). This proves that the *newly constructed representations are also representations in groups* $O_{\mathbb{K}}(N)$ (*and, with* $\mathbb{K} = \mathbb{R}$, *in groups* SO (N)).

Thus, for example, we have now represented the group Spin $(8m + 1)$ by orthogonal matrices of order 2^{4m} whereas earlier we represented it by unitary matrices of the same order. It is possible to show, however, by carefully examining all the isomorphisms that these *unitary matrices are in fact real* and that the resulting representation by real unitary, i.e. orthogonal, matrices is equivalent to that just constructed. (This follows without any calculations from the general results on matrix representations of groups Spin (n) which will be proved in the next semester course within the general theory of representations of compact Lie groups. Therefore we shall not prove this fact here.) Consequently we have in fact only one representation of the group Spin $(8m + 1)$ by orthogonal matrices. It is called a *spinor representation of the group.*

For group Spin $(8m)$ we now obtain a representation by pairs (A, B) of unimodular orthogonal matrices of order 2^{4m-1}. It turns out (which is again easiest to prove using the general theory to be developed in the next semester course) that on identifying these pairs with matrices (19) of order 2^{4m} we arrive at a representation equivalent to that constructed earlier. Thus here, too, we obtain only a slightly more refined representation of the previous representation.

However, it is more common to consider not pairs of matrices but components of those pairs individually, i.e. the two homomorphisms

$$\text{Spin}\,(8m) \rightrightarrows \text{SO}\,(2^{4m-1}). \tag{20}$$

These are called *semispinor representations* of group Spin $(8m)$.

It should be emphasized that *semispinor representations are not monomorphisms*. Indeed, under the isomorphism $\mathbb{C}l_\varepsilon(n) \approx \mathbb{C}l_{-\varepsilon}(n-2) \otimes \mathbb{C}l_\varepsilon(2)$ of Proposition 7 an element $e_{[n]} = e_1 \ldots e_n$ of $\mathbb{C}l_\varepsilon(n)$ goes over into an element $e_{[n-2]} \otimes (e_1e_2)^{n-1} = (-1)^{n-1} e_{[n-2]} \otimes 1$ of $\mathbb{C}l_{-\varepsilon}(n-2) \otimes \mathbb{C}l_\varepsilon(2)$. Therefore under an iterated isomorphism $\mathbb{C}l(n) \approx \mathbb{C}l(n-4) \otimes \mathbb{H}(2)$ (we restrict ourselves to the case $\varepsilon = -1$) that element goes over into $e_{n-4} \otimes E$, where E is the identity matrix. An induction now shows that given $n = 8m - 1$ the element $e_{[3]} \otimes E$ in $\mathbb{C}l(3) \otimes \mathbb{H}(2^{4m-3})$ and hence the element $e_1 \otimes 1 \otimes E \approx (E, -E)$ in $\mathbb{C}l_+(1) \otimes \mathbb{C}l(2) \otimes \mathbb{H}(2^{4m-3}) \approx (\mathbb{R} \otimes \mathbb{R}) \otimes \mathbb{R}(2^{4m-1})$ correspond to an element $e_{[n]}$. This proves that under one semispinor representation (20) an element $e_{[8m-1]}$ goes over into the identity matrix E and under the other, an element $-e_{[8m-1]}$ does. (It is assumed here that $\mathrm{Spin}(8m) \subset \mathbb{C}l(8m-1)$; under a natural embedding $\mathrm{Spin}(8m) \subset \mathbb{C}l^0(8m)$ there appears an element $e_{[8m]}$ instead of $e_{[8m-1]}$.) □

Remark 5. It can be shown that elements $e_{[8m]}$ and $-e_{[8m]}$ are the only nontrivial elements of a group Spin $(8m)$ that go over under homomorphisms (20) into an identity matrix.

The earlier constructed "paired" representation for a group Spin $(8m-1)$ can also be split into two homomorphisms. These, however, will be faithful representations (i.e. monomorphisms) and will be equivalent to a single new representation of the group Spin $(8m-1)$ in SO (2^{4m-1}).

For a group Spin $(8m-2)$ we now obtain a complex representation in a group U (2^{4m-2}). It turns out that under an embedding U $(2^{4m-2}) \subset$ SO (2^{4m-1}) it goes over into a representation equivalent to the representation constructed earlier in the group SO (2^{4m-1}).

For a group Spin $(8m-3)$ the earlier constructed representation is obtained in a similar fashion from the new quaternion representation.

For a group Spin $(8m+2)$ the quaternion representation constructed earlier turns out to be in fact a complex representation equivalent to the new representation. This situation is similar to that arising for $n = 8m + 1$.

For a group Spin $(8m+3)$ the "paired" quaternion representation constructed earlier consists of two representations equivalent to the new representation.

For a group Spin $(8m + 4)$ the quaternion representation constructed earlier turns out to be in fact a "block" representation reducing to a "paired" new representation.

In the last two cases the situation is similar to that for groups Spin $(8m - 1)$ and Spin $(8m)$, respectively.

As is already noted, all these statements follow easily from the general theory to be presented in the next semester's lectures. Their direct verification, though tiresome, is quite possible. It will be left to the reader.

We conclude this lecture by proving formula (18) from linear algebra which was taken above without proof. For the matrix of an operator A this formula is equivalent to a relation between its second-order minors and hence can be proved by a direct, though somewhat cumbersome, calculation. To elucidate the intrinsic significance of that formula, however, we prefer to give it here a more conceptual proof in its natural generality.

Let $\mathscr{V}$ be a finite-dimensional vector space over a field $\mathbb{K}$ and suppose as ever that $\mathscr{V}'$ is the conjugate space. Suppose further that $\bigwedge^p(\mathscr{V})$ and $\bigwedge^p(\mathscr{V}')$ are spaces of skew-symmetric p-linear functionals on $\mathscr{V}$ and $\mathscr{V}'$, respectively: see II, 9. For any p-vector $x_1 \wedge \ldots \wedge x_p \in \bigwedge^p(\mathscr{V})$ and any p-covector $\xi^1 \wedge \ldots \wedge \xi^p \in \bigwedge^p(\mathscr{V}')$ we put

$$(x_1 \wedge \ldots \wedge x_p, \xi^1 \wedge \ldots \wedge \xi^p) = \det |\, \xi^i(x_j) \,|_{i,j=1\ldots p}.$$

It can be easily checked that the function $\langle , \rangle$ by linearity can be correctly extended to any elements of vector spaces $\bigwedge^p(\mathscr{V})$ and $\bigwedge^p(\mathscr{V}')$ and is a pairing (see II, 4) between the spaces. Thus $\bigwedge^p(\mathscr{V})$ and $\bigwedge^p(\mathscr{V}')$ *are naturally dual to each other* and therefore the vector space $\bigwedge^p(\mathscr{V}') = \bigwedge_p(\mathscr{V})$ may be identified with a vector space $\bigwedge^p(\mathscr{V})'$ conjugate to $\bigwedge^p(\mathscr{V})$.

For every skew-symmetric functional $y \in \bigwedge^q(\mathscr{V})$ (it is now convenient for us to somewhat change the notation adopted in II) the correspondence $x \mapsto x \wedge y$, where $x \in \bigwedge^p(\mathscr{V})$, is a linear mapping $\bigwedge^p(\mathscr{V}) \to \bigwedge^{p+q}(\mathscr{V})$ and hence defines the conjugate mapping $\bigwedge^{p+q}(\mathscr{V}') \to \bigwedge^p(\mathscr{V}')$. The image of a functional $z \in \bigwedge^{p+q}(\mathscr{V}')$ under that mapping is denoted by $y \lrcorner z$ and called the *left internal product* of functionals y and z. By definition,

$$\langle x, y \lrcorner z \rangle = \langle x \wedge y, z \rangle \quad \text{for any} \quad z \in \bigwedge^{p+q}(\mathscr{V}').$$

Similarly, the *right internal product* $x \llcorner y$ of functionals $x \in \bigwedge^{p+q}(\mathscr{V})$ and $y \in \bigwedge^{q}(\mathscr{V}')$ is in $\bigwedge^{p}(\mathscr{V})$ and is characterized by the equation

$$\langle x \llcorner y, z\rangle = \langle x, y \wedge z\rangle \quad \text{for any} \quad z \in \bigwedge^{p}(\mathscr{V}').$$

If $e_1, \ldots, e_n$ is the basis of $\mathscr{V}$, then for any subset $I = \{i_1, \ldots, i_p\}$ of a set $[n] = \{1, \ldots, n\}$, where $i_1 < \ldots < i_p$, a basis p-vector $e_{i_1} \wedge \ldots \wedge e_{i_p}$ will be denoted by e_I (see a similar notation above for elements of a Clifford algebra). In a similar fashion e^I will denote a basis p-covector $e^{i_1} \wedge \ldots \wedge e^{i_p}$, where $e^1, \ldots, e^n$ are vectors of the conjugate basis of the space $\mathscr{V}'$. As it follows directly from the anticommutativity of external multiplication, for any subsets $I, J \subset [n]$ there is a formula

$$e_I \wedge e_J = \begin{cases} (-1)^{\tau(I, J)} e_{I\cup J}, & \text{if } I \cap J = \varnothing, \\ 0 & \text{otherwise,} \end{cases}$$

where $\tau(I, J)$, as in (13), is the number of pairs (i, j) for which $i \in I$, $j \in J$ and $i \geqslant j$. The same formula holds, of course, for the multi-covector $e^I \wedge e^J$.

It follows immediately from these formulas that

$$e_I \lrcorner e^J = \begin{cases} (-1)^{\tau(K, I)} e^K, & \text{if } I \subset J, \\ 0 & \text{otherwise,} \end{cases}$$

and similarly

$$e_J \llcorner e_I = \begin{cases} (-1)^{\tau(J, K)} e^K, & \text{if } I \subset J, \\ 0 & \text{otherwise,} \end{cases}$$

where $K = J \setminus I$ is the complement of I in J.

Consider now a linear operator $A: \mathscr{V} \to \mathscr{V}$. Setting for any multivector $x_1 \wedge \ldots \wedge x_p \in \bigwedge^p(\mathscr{V})$

$$A_{[p]}(x_1 \wedge \ldots \wedge x_p) = Ax_1 \wedge \ldots \wedge Ax_p,$$

and extending $A_{[p]}$ by linearity to any elements of the vector space $\bigwedge^p(\mathscr{V})$ we obviously define correctly some linear operator $A_{[p]}: \bigwedge^p(\mathscr{V}) \to \bigwedge^p(\mathscr{V})$ usually called the *p-th external degree* of the operator A. (The operator A considered above is nothing but an operator $A_{[2]}$.)

It is clear that

$$A_{[p+q]}(x \wedge y) = A_{[p]}x \wedge A_{[q]}y$$

for any functionals $x \in \Lambda^p(\mathscr{V})$ and $y \in \Lambda^q(\mathscr{V})$. In addition it follows immediately from the definitions that

$$(A')_{[p]} = (A_{[p]})',$$

where the prime designates as ever (see II, 14) the passage to the adjoint operator. Therefore the symbol $A'_{[p]}$ is quite correct.

The key to formula (10) is the following lemma:

Lemma 4. *For any functionals $x \in \Lambda^q(\mathscr{V})$, $y \in \Lambda^{p+q}(\mathscr{V}')$ and any operator $A: \mathscr{V} \to \mathscr{V}$ we have*

$$x \lrcorner A'_{[p+q]}y = A'_{[p]}(A_{[q]}x \lrcorner y).$$

Proof. For every functional $z \in \Lambda^p(\mathscr{V})$ we have

$$\begin{aligned}\langle z, x \lrcorner A'_{[p+q]}y\rangle &= \langle z \wedge x, A'_{[p+q]}y\rangle \\ &= \langle A_{[p+q]}(z \wedge x), y\rangle \\ &= \langle A_{[p]}z \wedge A_{[q]}x, y\rangle \\ &= \langle A_{[p]}z, A_{[q]}x \lrcorner y\rangle \\ &= \langle z, A'_{[p]}(A_{[q]}x \lrcorner y)\rangle. \quad \square\end{aligned}$$

We apply Lemma 4 to the case where $p + q = n$ and $y = e^{[n]} = e^1 \wedge \ldots \wedge e^n$. Since a direct calculation shows that

$$A'_{[n]}e^{[n]} = (\det A)\, e^{[n]},$$

by Lemma 3, for any functional $x \in \Lambda^q(\mathscr{V})$ and any operator $A: \mathscr{V} \to \mathscr{V}$ we have a formula

$$(\det A)(x \lrcorner e^{[n]}) = A'_{[p]}(A_{[q]}x \lrcorner e^{[n]}).$$

Putting

$$Tx = x \lrcorner e_{[n]}, \qquad x \in \Lambda^q(\mathscr{V}),$$

we can write this formula as follows

$$(\det A)\, T = A'_{[p]} \circ T \circ A_{[q]}, \quad \text{where} \quad p + q = n.$$

The mapping T is given in explicit form by the formula

$$Te_I = (-1)^{\tau(I)}e^J,$$

where $J = [n] \setminus I$ is the complement of I in $[n]$ and $\tau(I) = \tau(J, I)$ is the number of pairs (j, i) with $i \in I$, $j \notin I$ and $j \geqslant i$. In particular, it follows that T is an isomorphism $\Lambda^q(\mathscr{V}) \to \Lambda^{n-q}(\mathscr{V}')$.

In the special case, where $\det A = 1$ we obtain the formula

$$A^c_{[p]} \circ T = T \circ A_{[q]},$$

where $A^c = (A')^{-1}$.

So far all our constructions have been completely invariant (even the isomorphism T is independent of the choice of basis up to a constant factor since when changing the basis it is multiplied by the determinant of the transition matrix). Now, assuming the basis $e_1, \ldots, e_n$ to be chosen (i.e. going over, in fact, from the vector space $\mathscr{V}$ into the vector space $\mathbb{K}^n$) we identify $\mathscr{V}$ and $\mathscr{V}'$ using the equality of coordinates in the bases $e_1, \ldots, e_n$ and $e^1, \ldots, e^n$ (in invariant terms this is the same as giving in a vector space some scalar product, i.e. a pairing of that vector space with itself). Then T turns out to be an isomorphism $\Lambda^q(\mathscr{V}) \to \Lambda^{n-q}(\mathscr{V})$ and is defined by the formula

$$Te_I = (-1)^{\tau(I)} e_J$$

and hence, for $n = 4$, $p = q = 2$, coincides with the isomorphism T defined by formulas (17) (which are extended to the case of a ground field $\mathbb{K}$). Thus formula (18) turns out to be a special case of formula (21) to within notation.

Formula (18) may thus be considered to be completely proved.

Remark 6. Writing the general formula (21) in matrix form we obtain a formula expressing in terms of $q = n - p$ order minors of a nonsingular matrix p order minors of the inverse matrix. A purely computational proof of the formula is extremely cumbersome.

Lecture 14

Doubling of algebras · Metric algebras · Normed algebras · Automorphisms and differentiations of metric algebras · Differentiations of a doubled algebra · Differentiations and automorphisms of the algebra $\mathbb{H}$ · The algebra of octaves. The Lie algebra $\mathfrak{g}_2$ · Structural constants of the Lie algebra $\mathfrak{g}_2^{\mathbb{C}}$ · Representation of the Lie algebra $\mathfrak{g}_2^{\mathbb{C}}$ by generators and relations

The construction of quaternions from complex numbers is quite similar to the construction of complex numbers from reals. Moreover, both are special cases of the same general construction.

Let $\mathscr{A}$ be an arbitrary (but as ever finite-dimensional) algebra over the field of real numbers $\mathbb{R}$ in which a *conjugation*, i.e. some involutory antiautomorphism $a \mapsto \bar{a}$ (the case $\bar{a} = a$ for all $a \in \mathscr{A}$ is not excluded) is given.

Consider a vector space $\mathscr{A}^2$ which is a direct sum of two copies of a vector space $\mathscr{A}$, i.e. which consists of pairs of the form (a, b), where $a, b \in \mathscr{A}$. We introduce into $\mathscr{A}^2$ multiplication as follows:

$$(a, b)(u, v) = (au - \bar{v}b,\ b\bar{u} + va).$$

A simple check shows that relative to that multiplication the vector space $\mathscr{A}^2$ is an algebra (of dimension $2n$, where $n = \dim \mathscr{A}$). We shall call that algebra a *doubling* of the algebra $\mathscr{A}$.

Clearly, the correspondence $a \mapsto (a, 0)$ is a monomorphism of $\mathscr{A}$ into $\mathscr{A}^2$. We shall identify elements a and $(a, 0)$ and thus assume the algebra $\mathscr{A}$ to be a subalgebra of $\mathscr{A}^2$. If $\mathscr{A}$

is a unit algebra, then the element $1 = (1, 0)$ will obviously be an identity element in $\mathscr{A}^2$ too.

Let $e = (0, 1)$. Then $be = (0, b)$ and hence $(a, b) = a + be$ for any elements, $a, b \in \mathscr{A}$. Thus every element of algebra $\mathscr{A}^2$ is uniquely written as $a + be$, with

$$(1) \quad a(be) = (ba)e, \qquad (ae)b = (a\bar{b})e, \qquad (ae)(be) = -\bar{b}a,$$

which together with the distributivity requirement uniquely defines multiplication in $\mathscr{A}^2$. In particular $e^2 = -1$.

A doubling $\mathbb{R}^2$ of the field $\mathbb{R}$ is the algebra $\mathbb{C}$ of complex numbers and a doubling $\mathbb{C}^2$ of $\mathbb{C}$ is the algebra of quaternions $\mathbb{H}$. The first statement is obvious. To prove the second statement one should write out complex numbers in explicit form in every element $\xi = a + be$ of $\mathbb{C}^2$, i.e. put $a = a_0 + a_1 i$, $b = a_2 + a_3 i$, and denote e by j and ie by k. As a result we obtain for ξ the usual quaternion notation

$$\xi = a_0 + a_1 i + a_2 j + a_3 k.$$

The fact that i, j and $k = ij$ satisfy the usual quaternion identities is checked easily.

Since for any element a of $\mathscr{A}$ we have $ea = \bar{a}e$, the algebra $\mathscr{A}^2$ like the quaternion algebra $\mathbb{H}$, is deliberately noncommutative if the conjugation in $\mathscr{A}$ is not an identity mapping. In a similar fashion, since $a(be) = (ba)e$, the algebra $\mathscr{A}^2$ is nonassociative if $\mathscr{A}$ is noncommutative. In particular a *doubling* $\mathbb{H}^2$ *of the algebra* $\mathbb{H}$ *is nonassociative.*

Thus we see that as the construction of a doubling is iterated the algebraic properties of the multiplication gradually deteriorate.

Of course, for the construction of a doubling to be iterated it is necessary to define a conjugation in $\mathscr{A}^2$. We shall do this by the formula

$$\overline{a + be} = \bar{a} - be,$$

turning for $A = \mathbb{R}$ into the usual formula for complex conjugation (after replacing e by i of course). Clearly, this mapping is involutory and linear. A computation shows that it is simultaneously an antiautomorphism. For $\mathscr{A} = \mathbb{C}$ it is the usual conjugation in $\mathbb{H}$.

A unit algebra $\mathscr{A}$ over the field $\mathbb{R}$ is said to be a *metric*

algebra if a conjugation $a \mapsto \bar{a}$ is given in it such that given any element $a \in \mathcal{A}$ the element $a\bar{a}$ is in the space $\mathbb{R}$ (i.e., more precisely, in the subspace $\mathbb{R}\cdot 1$) and is positive for $a \neq 0$: $a\bar{a} > 0$. A real number $|a| = \sqrt{a\bar{a}}$ is called the *norm of a*. By definition, $|a| = 0$ if and only if $a = 0$.

A direct check shows that in any metric algebra $\mathcal{A}$ the formula

$$(x, y) = \frac{x\bar{y} + y\bar{x}}{2}$$

defines a scalar product. Thus, any metric algebra is a Euclidean space with respect to that product. The norm $|a|$ of an element $a \in \mathcal{A}$ is nothing but its length.

The orthogonal complement of the identity element in a metric algebra $\mathcal{A}$ is denoted by $\mathcal{A}'$.

Any element $a \in \mathcal{A}$ can be uniquely represented as $a = \lambda + a'$, where $\lambda \in \mathbb{R}$ and $a' \in \mathcal{A}'$. We have $\bar{a} = \lambda - a'$, so that, in particular, $a \in \mathcal{A}'$ *if and only if* $\bar{a} = -a$, *and* $a \in \mathbb{R}$ *if and only if* $\bar{a} = a$. By definition

$$x\bar{y} + \bar{x}y = 2\,(x, y) \tag{2}$$

for any elements x, y of the metric algebra $\mathcal{A}$. In particular, *if* $x, y \in \mathcal{A}'$, *then* $yx = -xy$ *if and only if* $x \perp y$.

It is easy to see that *given any metric algebra* $\mathcal{A}$ *the algebra* $\mathcal{A}^2$ *is also metric*. Indeed

$$(a + be)\,(\overline{a + be}) = (a + be)\,(\bar{a} - be) = a\bar{a} + b\bar{b}$$

for any element $a + be \in \mathcal{A}^2$. □

A scalar product in $\mathcal{A}^2$ is given as follows:

$$(a + be,\ u + ve) = (a, u) + (b, v),$$

so that the direct sum $\mathcal{A}^2 = \mathcal{A} \oplus \mathcal{A}$ turns out to be a direct sum of Euclidean spaces. Thus *all algebras* $\mathbb{R}$, $\mathbb{C} = \mathbb{R}^2$, $\mathbb{H} = \mathbb{C}^2$, $\mathbb{H}^2$, ... *are metric algebras.*

A finite-dimensional algebra $\mathcal{A}$ which is at the same time a Euclidean space (but not necessarily a metric one a priori) is said to be a *normed algebra* if

$$|ab| = |a|\cdot|b|$$

for any elements $a, b \in \mathcal{A}$. In such an algebra, for any element $a \neq 0$ the mappings $x \mapsto \dfrac{ax}{|a|}$ and $x \mapsto \dfrac{xa}{|a|}$ are isometric

and hence ($\mathcal{A}$ being a finite-dimensional algebra) bijective. Therefore for any element $b \in \mathcal{A}$ the equations $ax = b$ and $xa = b$ are uniquely solvable in $\mathcal{A}$, i.e. the *normed algebra* $\mathcal{A}$ *is a division algebra.*

Examples of normed algebras are metric algebras $\mathbb{R}$, $\mathbb{C}$ and $\mathbb{H}$. As we shall see below, the metric algebra $\mathbb{H}^2$ is also normed.

Hurwitz's theorem to be proved in Semester VI says that there are no normed algebras other than those four algebras (so that, in particular, any normed algebra is necessarily a metric algebra).

If an automorphism $\Phi: \mathcal{A} \to \mathcal{A}$ of a matric algebra is commutative with a conjugation (i.e. if $\overline{\Phi a} = \Phi \bar{a}$ for any element $a \in A$), then it is of course an orthogonal operator. Conversely, if an automorphism $\Phi: \mathcal{A} \to \mathcal{A}$ of a metric algebra $\mathcal{A}$ is orthogonal, then since $\Phi 1 = 1$ it sends to itself the subspace $\mathcal{A}'$ and is therefore commutative with the conjugation.

And it is easy to see that if $\mathcal{A}$ *is a normed algebra, then any automorphism* $\Phi: \mathcal{A} \to \mathcal{A}$ *of it is an orthogonal operator.* Indeed it suffices to prove (see II, 21, condition (b) of Proposition 2) that if $|a| = 1$, then $|\Phi a| = 1$. But if $|\Phi a| < 1$, then $|\Phi a^k| = |(\Phi a)^k| = |\Phi a|^k \to 0$ as $k \to \infty$, i.e. $\Phi a^k \to 0$ and hence $a^k \to 0$. Therefore $|a|^k = |a^k| \to 0$, which is impossible for $|a| = 1$. Similarly, if $|\Phi a| > 1$, then $|a|^k \to \infty$ as $k \to \infty$, which is also impossible. Hence $|\Phi a| = 1$. $\square$

As a rule some basis is fixed in all our algebras $\mathcal{A}$. Therefore the group of orthogonal perators $\mathcal{A} \to \mathcal{A}$ can be identified with the group $O(n)$ of orthogonal matrices. By virtue of this identification, for the group Aut $\mathcal{A}$ of automorphisms of a normed algebra $\mathcal{A}$ there is an inclusion

$$\text{Aut}\, \mathcal{A} \subset O(n), \quad \text{where} \quad n = \dim \mathcal{A}.$$

Moreover, since every automorphism $\Phi: \mathcal{A} \to \mathcal{A}$ can be uniquely defined by the linear mapping $\Phi': \mathcal{A}' \to \mathcal{A}'$ (if $a = \lambda + a'$, where $\lambda \in \mathbb{R}$ and $a' \in \mathcal{A}'$, then $\Phi a = \lambda + \Phi' a'$), we may assume identifying Φ with Φ' that

$$\text{Aut}\, \mathcal{A} \subset O(n - 1). \tag{3}$$

In particular, it is true for $\mathcal{A} = \mathbb{C}$ when $n = 2$. Consequent-

ly, since $O(1) = \mathbb{Z}_2$ *the group* Aut $\mathbb{C}$ *is a second-order group* $\mathbb{Z}_2$ *consisting of an identity automorphism* id *and an automorphism of a complex conjugation* $a \mapsto \bar{a}$.

For the Lie algebra Der $\mathcal{A} = \mathfrak{l}$ (Aut $\mathcal{A}$), of differentiations of the algebra $\mathcal{A}$, it follows from inclusion (3) that

$$\text{Der}\,\mathcal{A} \subset \mathfrak{so}\,(n-1), \tag{4}$$

where $\mathfrak{so}\,(n-1)$ is a Lie algebra of skew-symmetric $n-1$ order matrices. Therefore, in particular, Der $\mathbb{C} = 0$.

However, equations Aut $\mathbb{C} = \mathbb{Z}_2$ and Der $\mathbb{C} = 0$ are easy to obtain also in a straightforward way. Indeed, being a linear operator over the field $\mathbb{R}$ which sends 1 to 1, any automorphism $\Phi\colon \mathbb{C} \to \mathbb{C}$ is uniquely defined by a number Φi. But since $i^2 = -1$, there must be an equation $(\Phi i)^2 = -1$ for that number. Hence $\Phi i = \pm i$, which just gives us an identity operator and a complex conjugation.

Similarly, any differentiation $D\colon \mathbb{C} \to \mathbb{C}$ is uniquely defined by a number Di which must satisfy the identity

$$Di\cdot i + i\cdot Di = D\,(i^2) = -D1 = 0$$

that is possible only when $Di = 0$.

These simple considerations allow a generalization to the case of any doubled algebra $\mathcal{A}^2$. Namely, every differentiation D of an algebra $\mathcal{A}^2$ defines by the formulas

$$Da = D_0a + Fa\cdot e, \quad De = x_0 + y_0e$$

two linear operators D_0, $F\colon \mathcal{A} \to \mathcal{A}$ and two elements x_0, $y_0 \in \mathcal{A}$, with the differentiation D being uniquely recovered from D_0, F and x_0, y_0 in view of the equation

$$D\,(a + be) = Da + Db\cdot e + b\cdot De,$$

i.e. the equation

$$D\,(a + be) = (D_0a - Fb + bx_0) + (Fa + D_0b + y_0b)\,e. \tag{5}$$

To describe the Lie algebra Der $\mathcal{A}^2$ therefore it suffices to describe quadruples (D_0, F, x_0, y_0) for which formula (5) gives the differentiation of the algebra $\mathcal{A}^2$. (In a similar fashion we can describe automorphisms, but this leads to complicated calculations.)

To obtain conditions on D_0, F, x_0, y_0 ensuring the inclusion $D \in$ Der $\mathcal{A}^2$ it is necessary that in the relation

(6) $$D(\xi\eta) = D\xi\cdot\eta + \xi\cdot D\eta,$$

where $\xi = a + be$ and $\eta = x + ye$ are elements in $\mathcal{A}^2$, D should be expressed in terms of (5), all multiplications should be carried out and the coefficients of 1 and e at the left and right should be compared. For example, at $\xi = a$, $\eta = x$ we obtain the identity

$$D_0(ax) + F(ax)e = (D_0a\cdot x + a\cdot D_0x) + (Fa\cdot\bar{x} + Fx\cdot a)e$$

from which it follows that D_0 is a differentiation of the algebra $\mathcal{A}$ and F satisfies the identity

(7) $$F(ax) = Fa\cdot\bar{x} + Fx\cdot a.$$

Similar identities can be obtained at $\xi = be$ and $\eta = x$, at $\xi = a$ and $\eta = ye$, at $\xi = be$ and $\eta = ye$. It turns out in practice, however, that it is appropriate to find first a general solution of the functional equation (7) and then consider these supplementary identities. Besides, it is useful to consider from the outset relations $x_0 + \bar{x}_0 = 0$ and $y_0 + \bar{y}_0 = 0$ resulting at $\xi = \eta = e$ and implying that $x_0, y_0 \in A'$.

Suppose, for example, $\mathcal{A} = \mathbb{C}$ and hence $\mathcal{A}^2 = \mathbb{H}$. Since $\operatorname{Der}\mathbb{C} = 0$, we have $D_0 = 0$. To calculate the operator F, we can use the fact that $\mathbb{C} = \mathbb{R}^2$, and apply the same method by introducing linear operators $P, Q: \mathbb{R} \to \mathbb{R}$ defined by

$$Fx = Px + Qx\cdot i, \quad x \in \mathbb{R}.$$

For $a, x \in \mathbb{R}$, it follows from identity (7) that

$$P(ax) = Pa\cdot x + Px\cdot a \quad\text{and}\quad Q(ax) = Qa\cdot x + Qx\cdot a,$$

i.e. that P and Q are differentiations of the field $\mathbb{R}$. Therefore $P = Q = 0$, i.e. $Fx = 0$ for $x \in \mathbb{R}$. Hence $F(x + yi) = F(yi) = Fi\cdot y$, i.e.

$$Fa = z_0\cdot\operatorname{Im} a, \quad\text{where}\quad z_0 = Fi.$$

A direct check shows that relation (7) holds for all z_0. This proves that any differentiation $D: \mathbb{H} \to \mathbb{H}$ must be (see formula (5)) of the form

(8) $$D(a + bj) = (-z_0\operatorname{Im} b + bx_0) + (z_0\operatorname{Im} a + y_0b)j,$$

where $x_0, y_0, z_0 \in \mathbb{C}$. Parameters x_0 and y_0 must be in $\mathbb{C}'$, i.e. be of the form $x_0 = ia_0$, $y_0 = ib_0$, where $a_0, b_0 \in \mathbb{R}$. Substituting the obtained expression in the general formula (6) we now at once discover that the mapping $D: \mathbb{H} \to \mathbb{H}$ given by formula (8) is a differentiation of the algebra $\mathbb{H}$ if and only if $\operatorname{Re} z_0 = -a_0$, i.e. $z_0 = -a_0 + ic_0$, where $c_0 \in \mathbb{R}$. This proves that *every differentiation $D: \mathbb{H} \to \mathbb{H}$ of the algebra $\mathbb{H}$ is given by the formula*

$$(9)\qquad \begin{aligned} D(a + bj) &= i(a_0 \operatorname{Re} b - c_0 \operatorname{Im} b) \\ &+ [-(a_0 \operatorname{Im} a + b_0 \operatorname{Im} b) + i(b_0 \operatorname{Re} b + c_0 \operatorname{Im} a)]\, j, \end{aligned}$$

where a_0, b_0, c_0 are real numbers.

Mapping (9) sends the subspace $\mathbb{H}'$ to itself and is given by the matrix

$$\begin{pmatrix} 0 & a_0 & -c_0 \\ -a_0 & 0 & -b_0 \\ c_0 & b_0 & 0 \end{pmatrix}$$

in the basis i, j, k of that subspace.

Thus $\operatorname{Der} \mathbb{H} \subset \mathfrak{so}(3)$ according to the general formula (4). Moreover, we now see that

$$\operatorname{Der} \mathbb{H} = \mathfrak{so}(3).$$

For the group $\operatorname{Aut} \mathbb{H}$, it follows from this equation that this group coincides either with a group $SO(3)$ or with a group $O(3)$ (since by the general formula (3) there is an inclusion $\operatorname{Aut} \mathbb{H} \subset O(3)$). Since a mapping with a matrix $-E$ is obviously not an automorphism, we have

$$(10)\qquad \operatorname{Aut} \mathbb{H} = SO(3).$$

In particular, we see that unlike $\operatorname{Aut} \mathbb{C}$ the *group* $\operatorname{Aut} \mathbb{H}$ *is connected.*

Besides, comparing equation (10) with Proposition 4 of Lecture 13 we immediately see that *any automorphism $\mathbb{H} \to \mathbb{H}$ is an internal automorphism of the form $\eta \mapsto \xi\eta\xi^{-1}$*, where $\xi \in S^3$.

Remark 1. In fact equation (10) can be proved without any calculations if we use Proposition 4 of Lecture 13. Indeed, that proposition means that the group of internal

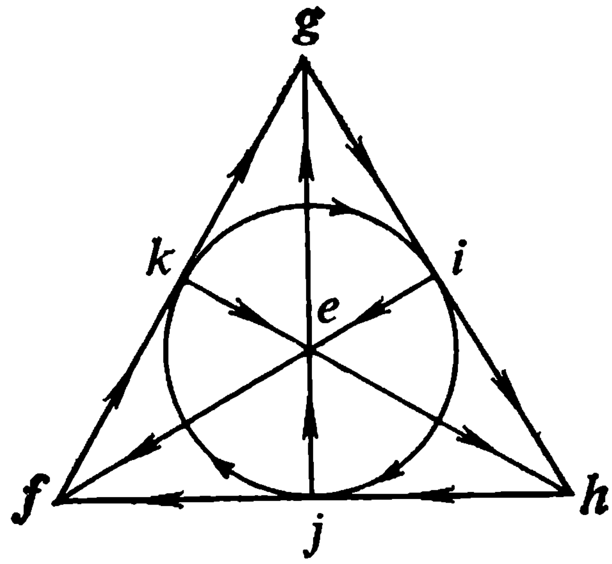
automorphisms $\eta \mapsto \xi\eta\xi^{-1}$, $\xi \in S^3$ of the algebra $\mathbb{H}$ coincides with SO (3). Hence Aut $\mathbb{H} \supset$ SO (3). On the other hand, as we have just shown, the equation Aut $\mathbb{H} =$ O (3) is impossible. Therefore Aut $\mathbb{H} =$ SO (3). We have nevertheless given here a direct proof since it will serve us as a pattern for the more complicated case of the algebra $\mathbb{H}^2$.

The algebra $\mathbb{H}^2$ is called an *algebra of octaves* (or an *algebra of Cayley numbers or a Cayley algebra*). Its elements are *octaves* (or *Cayley numbers*). It is common to denote this algebra by $\mathbb{C}$a, in honour of Cayley although Cayley was not the first to discover it (it was Graves).

By definition every octave is of the form $\xi = a + be$, where a and b are quaternions and octaves are multiplied using formulas (1). The basis of $\mathbb{C}$a consists of 1 and seven elements

(11) $\quad i,\ j,\ k,\ e,\ f = ie, \qquad g = je, \qquad h = ke,$

the square of each of which is -1 and their pairwise products are diagrammatically represented by the following picture:



The product of any two elements (11) is equal up to a sign to the element on the same straight line (or the circle) and the sign is determined by the orientation of that line. For example, $eh = k$ and $fj = -h$.

As already noted, the algebra $\mathbb{C}$a is nonassociative. *It is alternative*, however, i.e. for any two of its elements, ξ and η, we have the identities

$$(\xi\eta)\,\eta = \xi\,(\eta\eta), \qquad \xi\,(\xi\eta) = (\xi\xi)\,\eta.$$

Indeed, let $\xi = a + be$, $\eta = u + ve$. Then

$$\xi\eta = (au - \bar{v}b) + (b\bar{u} + va)\,e,$$

$$(\xi\eta)\,\eta = [(au - \bar{v}b)\,u - \bar{v}\,(b\bar{u} + va)] + [(b\bar{u} + va)\,\bar{u} + v\,(au - \bar{v}b)]\,e,$$

$$\eta\eta = (u^2 - \bar{v}v) + (v\bar{u} + vu)\,e,$$

$$\xi\,(\eta\eta) = [a\,(u^2 - \bar{v}v) - \overline{(v\bar{u} + vu)}\,b] + [b\,\overline{(u^2 - \bar{v}v)} + (v\bar{u} + vu)\,a]\,e,$$

and since the numbers $\bar{v}v = v\bar{v}$ and $u + \bar{u}$ are real and so commute with any quaternion we have

$$\begin{aligned} a\,(u^2 - \bar{v}v) - \overline{(v\bar{u} + vu)}\,b &= au^2 - a\bar{v}v - (u + \bar{u})\,\bar{v}b \\ &= au^2 - \bar{v}va - \bar{v}b\,(u + \bar{u}) \\ &= (au - \bar{v}b)\,u - \bar{v}\,(b\bar{u} + va), \end{aligned}$$

$$\begin{aligned} b\,\overline{(u^2 - \bar{v}v)} + (v\bar{u} + vu)\,a &= b\bar{u}^2 - b\bar{v}v + v\,(\bar{u} + u)\,a \\ &= b\bar{u}^2 - v\bar{v}b + va\,(\bar{u} + u) \\ &= (b\bar{u} + va)\,\bar{u} + v\,(au - \bar{v}b). \end{aligned}$$

Therefore $(\xi\eta)\,\eta = \xi\,(\eta\eta)$.

The equation $\xi\,(\xi\eta) = (\xi\xi)\,\eta$ can be proved similarly. □

According to the general theory the conjugation in $\mathbb{C}\mathrm{a}$ is given as follows:

$$\overline{a + be} = \bar{a} - be.$$

It leaves the element 1 fixed and changes the sign of each element (11), so that elements (11) make up a basis of a subspace $\mathbb{C}\mathrm{a}'$.

As shown by Artin, in an alternative algebra any two elements generate an associative subalgebra. The same reasoning therefore as that for quaternions shows that the *octave algebra* $\mathbb{C}\mathrm{a}$ *is normed.* The proof of Artin's theorem is rather cumbersome, however, and we have no time to spare. Therefore we prove that $\mathbb{C}\mathrm{a}$ is a normed algebra by direct calculation.

Let $\xi = a + be$ and $\eta = u + ve$ be two octaves. We must prove that $|\,\xi\eta\,| = |\,\xi\,|\cdot|\,\eta\,|$. But according to the fore-

going

$$| \xi\eta |^2 = | au - v\bar{b} |^2 + | b\bar{u} + va |^2$$
$$= (au - \bar{v}b)\,\overline{(\bar{u}a - \bar{b}v)} + (b\bar{u} + va)\,(u\bar{b} + \bar{a}\bar{v}),$$
$$| \xi |^2 \, | \eta |^2 = (a\bar{a} + b\bar{b})\,(u\bar{u} + v\bar{v}).$$

Assuming $v = \lambda + v'$, where $\lambda \in \mathbb{R}$ and $v' \in \mathbb{C}\mathrm{a}'$ (and hence $\bar{v}' = -v'$), we therefore get

$$\begin{aligned} | \xi\eta |^2 - | \xi |^2 \, | \eta |^2 = \lambda\,(a\bar{u}b + \bar{b}\bar{u}\bar{a} - \bar{b}ua - a\bar{u}b) \\ + (a\bar{u}b + \overline{bua})\,v' \\ - v'\,(\bar{a}\bar{u}\bar{b} + \bar{b}\bar{u}\bar{a}) = 0, \end{aligned}$$

for $a\bar{u}b + \bar{b}\bar{u}\bar{a}$ is a real number and therefore commutes with the quaternion v'. □

In particular, it follows that $\mathbb{C}\mathrm{a}$ *is a division algebra.* However, as in the case of quaternions, it can be directly checked (using alternativity) that equations $\xi x = \eta$ and $x\xi = \eta$ are satisfied (for $\xi \neq 0$) respectively by the octaves $x = \xi^{-1}\eta$ and $x = \eta\xi^{-1}$, where $\xi^{-1} = \dfrac{\bar{\xi}}{| \xi |^2}$. □

Remark 2. Since the construction of a doubling can be indefinitely iterated, there arise metric algebras $\mathbb{C}\mathrm{a}^2$, $(\mathbb{C}\mathrm{a}^2)^2$, . . ., etc. But these algebras are of little interest, being neither normed (by virtue of the Hurwitz theorem) nor alternative (by virtue of the so-called *generalized Frobenius theorem* every alternative finite-dimensional algebra over the field $\mathbb{R}$ is isomorphic to one of the algebras $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$ or $\mathbb{C}\mathrm{a}$; see [12], for example). Moreover, the algebras are even not division algebras since using very powerful tools of modern algebraic topology one can prove (it was Adams who was the first to do so) that the dimension of a division algebra over $\mathbb{R}$ can have only the values 1, 2, 4 and 8 (there are division algebras of dimensions 4 and 8 distinct from algebras $\mathbb{H}$ and $\mathbb{C}\mathrm{a}$).

For reasons we cannot now go into the group of automorphisms $\mathrm{Aut}\,\mathbb{C}\mathrm{a}$ of an algebra $\mathbb{C}\mathrm{a}$ is denoted by G_2 and its Lie algebra $\mathrm{Der}\,\mathbb{C}\mathrm{a}$ is by $\mathfrak{g}_2$ accordingly. Since $\mathbb{C}\mathrm{a}$ is normed and $\dim \mathbb{C}\mathrm{a} = 8$, according to (3)

$$G_2 \subset \mathrm{O}(7)$$

and hence

$$\mathfrak{g}_2 \subset \mathfrak{so}\,(7),$$

where $\mathfrak{so}\,(7)$ is a Lie algebra of skew-symmetric matrices of the seventh order.

Unlike the preceding case, however, the algebra $\mathfrak{g}_2$ does not coincide with $\mathfrak{so}\,(7)$, so that now we deal with some *new* Lie algebra (and new Lie group) we have not yet encountered. We prove that by calculating the dimension of $\mathfrak{g}_2$ which turns out to be 14 (whereas $\dim \mathfrak{so}\,(7) = 21$).

The calculation of $\mathfrak{g}_2$ is made by the method we already know. Every differentiation $D \in \mathfrak{g}_2$ is given by formula (5), where now x_0 and y_0 are quaternions, D_0 is some differentiation of the algebra $\mathbb{H}$ and F is a linear operator $\mathbb{H} \to \mathbb{H}$ satisfying identity (7). Assuming $Fx = Px + Qx \cdot j$, where $x \in \mathbb{C}$ and P and Q are linear operators $\mathbb{C} \to \mathbb{C}$, we obtain, for P and Q, equations

$$P\,(xy) = Px \cdot \bar{y} + Py \cdot x, \qquad Q\,(xy) = Qx \cdot y + Qy \cdot \bar{x}$$

whose general solution is of the form

$$Px = a_0 \operatorname{Im} x, \qquad Qx = b_0 \operatorname{Im} x,$$

where $a_0, b_0 \in \mathbb{C}$. Hence putting $Fj = z_0 + w_0 j$, where $x_0, w_0 \in \mathbb{C}$, we see that a general solution of the functional equation (5) in $\mathbb{H}$ is of the form

$$\begin{aligned} F\xi &= (a_0 \operatorname{Im} x + b_0 \operatorname{Im} y + z_0 y) \\ &\quad + (b_0 \operatorname{Im} x - a_0 \operatorname{Im} y + \omega_0 \bar{y})\, j, \\ \xi &= x + yj, \end{aligned} \tag{12}$$

where $a_0, b_0, z_0, w_0 \in \mathbb{C}$. A rather tedious, calculation now shows that the mapping $D\colon \mathbb{C}\mathrm{a} \to \mathbb{C}\mathrm{a}$ defined by formula (5), where D_0 is some differentiation of $\mathbb{H}$, while F is mapping (12) and x_0 and y_0 are quaternions in H', is a differentiation of $\mathbb{C}\mathrm{a}$, i.e. is in $\mathfrak{g}_2$, if and only if $x_0 = -i \operatorname{Re} a_0 - (\bar{z}_0 + i \operatorname{Re} b_0)\, j$.

This proves the following lemma:

Lemma 1. *Every differentiation D of a Cayley algebra $\mathbb{C}\mathrm{a}$ is given by:*

(a) *a differentiation D_0 of the quaternion algebra $\mathbb{H}$;*

(b) *a quaternion y_0 satisfying the relation $\bar{y}_0 = -y_0$;*

(c) *four complex numbers* a_0, b_0, z_0, w_0.

That differentiation acts by the formula

$$D(\xi + \eta e) = (D_0\xi - F\eta + \eta x_0) + (F\xi + D_0\eta + y_0\eta)\, e,$$

where F *is a mapping* $\mathbb{H} \to \mathbb{H}$ *defined by formula* (12) *and* $x_0 = -i \operatorname{Re} a_0 - (\overline{z_0} + i \operatorname{Re} b_0)\, j$. □

A differentiation D_0 is given by a skew-symmetric matrix of order 3 and hence depends on three real parameters, the quaternion y_0 also depends on three parameters and the quadruple a, b, x_0, y_0 depends on eight parameters. Therefore the differentiation D is defined by giving $14 = 3 + 3 + 8$ independent real parameters. Hence $\dim \mathfrak{g}_2 = 14$.

In basis (11) a differentiation D is given by a matrix that can be represented in the following conventional but clear form

$$\begin{array}{c|ccc|c|c|}
 & i & j & k & e \quad f & g \quad h \\ \hline
i & & & & -a_0 & -b_0 \\
j & & D_0 & & -z_0 & -w_0 \\
k & & & & -c_0 & d_0 \\ \hline
e,\ f & a_0 & z_0 & c_0 & 0 & -y_0 \\
g,\ h & b_0 & w_0 & -d_0 & y_0 & D_0 + \dot{y}_0 \\ \hline
\end{array}$$

where $c_0 = b_0 + z_0 i$, $d_0 = a_0 + w_0 i$ and $\dot{y}_0$ denotes an operator (from $\mathbb{H}'$ to $\mathbb{H}$) of multiplication by y_0. (The operator has a matrix

$$\begin{pmatrix} -b_1 & -b_2 & -b_3 \\ 0 & -b_3 & b_2 \\ b_3 & 0 & -b_1 \\ -b_2 & b_1 & 0 \end{pmatrix},$$

where $b_1 i + b_2 j + b_3 k = y_0$). It follows that matrices in $\mathfrak{g}_2$ are characterized among all skew-symmetric matrices

(a_{ij}) of order 7 by the following seven conditions:

$$
\begin{array}{lll}
 & a_{32} + a_{45} + a_{76} = 0, & \\
 & a_{13} + a_{64} + a_{75} = 0, & a_{21} + a_{65} + a_{47} = 0, \\
(13) & a_{14} + a_{36} + a_{27} = 0, & a_{51} + a_{26} + a_{73} = 0, \\
 & a_{17} + a_{42} + a_{53} = 0, & a_{61} + a_{52} + a_{34} = 0.
\end{array}
$$

If $a_0 = b_0 = 0$ and

$$
D_0 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & p \\ 0 & -p & 0 \end{pmatrix},
$$

i.e. if $Di = 0$, then the differentiation D will send to itself a subspace $\mathscr{V}'$ of $\mathbb{C}a$ orthogonal to the elements 1 and i. That subspace is closed under multiplication by i and can therefore be considered as a vector space over $\mathbb{C}$ with a basis j, e, g. A direct calculation now shows that in that basis the differentiation D is given by the complex matrix

$$
\begin{pmatrix} -pi & -\bar{z}_0 & -v_0 \\ z_0 & b_1 i & -v_0 \\ \bar{v}_0 & \bar{v}_0 & (p - b_1) i \end{pmatrix},
$$

where $v_0 = b_2 + b_3 i$ and p and b_1 are real numbers. Since this is precisely the general form of skew-symmetric matrices of order 3 with a trace equal to zero, we see that *differentiations D: $\mathbb{C}a \to \mathbb{C}a$ for which $Di = 0$ constitute a subalgebra of $\mathfrak{g}_2$ which is isomorphic to a Lie algebra $\mathfrak{su}(3)$.*

The standard way of describing any finite-dimensional algebras is giving in some basis their *structural constants*, i.e. the coefficients of decompositions with respect to pairwise products of the elements of that basis. Thus if $e_1, \ldots, e_n$ is the basis of an algebra $\mathscr{A}$, then its structural constants c_{ij}^k are defined by the formula

$$
e_i e_j = c_{ij}^k e_k, \qquad i, j, k = 1, \ldots, n.
$$

The general number of those constants is n^3.

As applied to the Lie algebra $\mathfrak{g}_2$ this method requires indicating $2744 = 14^3$ numbers, which of course is impracticable. The situation is not improved by the skew-symmetry

of the constants with respect to i and j since even then there remain $1279 = 91 \cdot 14 = \frac{14 \cdot 13}{2} \cdot 14$ constants. There is hope, however, that with an appropriate choice of basis these constants would exhibit certain regularities allowing them to be described in a satisfactory manner. It turns out that this can be really attained, the situation becoming especially simple after the complexification of the Lie algebra $\mathfrak{g}_2$, i.e. for the Lie algebra $\mathfrak{g}_2^{\mathbb{C}} = \mathfrak{g}_2 \otimes \mathbb{C}$ over the field $\mathbb{C}$, which consists of complex matrices of order 7 satisfying conditions (13). Since going back from $\mathfrak{g}_2^{\mathbb{C}}$ to $\mathfrak{g}_2$ is easy to check, this gives us structural constants also for $\mathfrak{g}_2$.

Consider the standard basis of the Lie algebra $\mathfrak{so}(7)$ consisting of matrices

$$E_{[i,j]} = \frac{E_{ij} - E_{ji}}{2},$$

where $i, j = 1, \ldots, 7$ and $i < j$. It follows directly from conditions (13) that all matrices

$$\begin{aligned}
P_0 &= E_{[3,2]} + E_{[6,7]}, & Q_0 &= E_{[4,5]} + E_{[6,7]},\\
P_1 &= E_{[1,3]} + E_{[5,7]}, & Q_1 &= E_{[6,4]} + E_{[5,7]},\\
P_2 &= E_{[2,1]} + E_{[7,4]}, & Q_2 &= E_{[6,5]} + E_{[7,4]},\\
P_3 &= E_{[1,4]} + E_{[7,2]}, & Q_3 &= E_{[3,6]} + E_{[7,2]},\\
P_4 &= E_{[5,1]} + E_{[3,7]}, & Q_4 &= E_{[2,6]} + E_{[3,7]},\\
P_5 &= E_{[1,7]} + E_{[3,5]}, & Q_5 &= E_{[4,2]} + E_{[3,5]},\\
P_6 &= E_{[6,1]} + E_{[4,3]}, & Q_6 &= E_{[5,2]} + E_{[4,3]}
\end{aligned}$$

are in $\mathfrak{g}_2$. Since these matrices are linearly independent, they constitute a basis (over the field $\mathbb{R}$) of the Lie algebra $\mathfrak{g}_2$.

Particular attention will be paid to linear combinations

$$H = aP_0 + bQ_0 = aE_{[3,2]} + bE_{[4,5]} + cE_{[7,6]} \tag{14}$$

of matrices P_0 and Q_0, where $a + b + c = 0$. Notice that $[H_1, H_2] = 0$ for any elements H_1 and H_2 of the form (14).

A direct calculation with matrices shows that

$$\begin{aligned}
[H, P_1] &= aP_2 + cQ_2, & [H, Q_1] &= (c - b)Q_2,\\
[H, P_2] &= -aP_1 - cQ_1, & [H, Q_2] &= (b - c)Q_1,
\end{aligned}$$

$$[H, P_3] = bP_4 + cQ_4, \qquad [H, Q_3] = (c-a)\,Q_4,$$
$$[H, P_4] = -bP_3 - cQ_3, \qquad [H, Q_4] = (a-c)\,Q_3,$$
$$[H, P_5] = cP_6 + aQ_6, \qquad [H, Q_5] = (a-b)\,Q_6,$$
$$[H, P_6] = -cP_5 - aQ_5, \qquad [H, Q_6] = (b-a)\,Q_5,$$

from which it follows at once that the elements

$$U_{\pm 1} = (2P_2 - Q_2) \pm i\,(2P_1 - Q_2), \qquad V_{\pm 1} = Q_2 \pm iQ_1,$$
$$U_{\pm 2} = (2P_4 - Q_4) \pm i\,(2P_3 - Q_3), \qquad V_{\pm 2} = Q_4 \pm iQ_3,$$
$$U_{\pm 3} = (2P_6 - Q_6) \pm i\,(2P_5 - Q_5), \qquad V_{\pm 3} = Q_6 \pm iQ_5$$

which constitutes the basis of the complexified algebra $\mathfrak{g}_2^{\mathbb{C}}$ satisfy the relations

$$\begin{aligned} &[H, U_{\pm 1}] = \pm iaU_{\pm 1}, && [H, V_{\pm 1}] = \pm i\,(c-b)\,V_{\pm 1}, \\ (15)\quad &[H, U_{\pm 2}] = \pm ibU_{\pm 1}, && [H, V_{\pm 2}] = \pm i\,(c-a)\,V_{\pm 2}, \\ &[H, U_{\pm 3}] = \pm icU_{\pm 3}, && [H, V_{\pm 3}] = \pm i\,(a-b)\,V_{\pm 3}. \end{aligned}$$

To write these relations more compactly, it is appropriate to introduce a two-dimensional real space $\mathfrak{h}^*$ conjugate to the two-dimensional space $\mathfrak{h}$ of all elements of the form (14). Let e_1, e_2 be a basis of $\mathfrak{h}^*$ conjugate to the basis P_0, Q_0 of $\mathfrak{h}$. Then for every element (14) of $\mathfrak{h}$ there are formulas

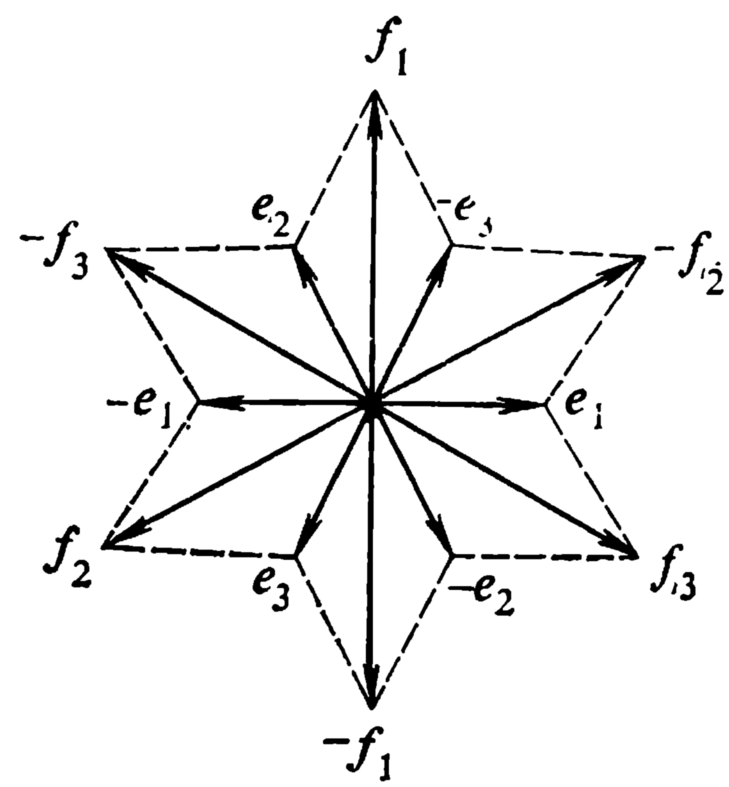
$$16) \qquad e_1(H) = a, \qquad e_2(H) = b, \qquad e_3(H) = c,$$

where $e_3 = -(e_1 + e_2)$.

It is convenient (though not obligatory) to assume that a Euclidean structure and rectangular coordinates in which vectors e_1 and e_2 have coordinates $\left(\frac{\sqrt{6}}{3}, 0\right)$ and $\left(\frac{-\sqrt{6}}{6}, \frac{\sqrt{2}}{2}\right)$ respectively are introduced into $\mathfrak{h}^*$. Then the vectors $\pm e_1$, $\pm e_2$, $\pm e_3$ together with $\pm f_1$, $\pm f_2$, $\pm f_3$, where

$$f_1 = e_2 - e_3, \qquad f_2 = e_3 - e_1, \qquad f_3 = e_1 - e_2$$

are radius vectors of the vertices of a regular star-shaped dodecagon. The collection of these twelve vectors in a plane will be called a *configuration* G_2.



We associate now with every vector $\alpha \in G_2$ an element X_α of the Lie algebra $\mathfrak{g}_2^{\mathbb{C}}$, putting

$$X_\alpha = \begin{cases} U_{\pm k} & \text{if} \quad \alpha = \pm e_k, \\ V_{\pm k} & \text{if} \quad \alpha = \pm f_k. \end{cases}$$

In view of relations (16) formulas (15) can then be written as the following single formula:

$$[H, X_\alpha] = i\alpha(H) X_\alpha. \tag{17}$$

Elements X_α, $\alpha \in G_2$, together with any pair H_1, H_2 of linearly independent elements of $\mathfrak{h}$ constitute a basis of $\mathfrak{g}_2^{\mathbb{C}}$. Since by construction $\bar{X}_\alpha = X_{-\alpha}$, the basis of $\mathfrak{g}_2$ will be made up of the elements H_1, H_2 and elements $X_\alpha + X_{-\alpha}$, $\frac{1}{i}(X_\alpha - X_{-\alpha})$. Since the structural constants of the last basis can be expressed in terms of the structural constants of the basis H_1, H_2, X_α, it is sufficient for us to find only the latter. Since the brackets $[H_1, X_\alpha]$ and $[H_2, X_\alpha]$ are directly calculated by formula (17) and the bracket $[H_1, H_2]$ is known to be zero, all we thus need is to calculate the brackets $[X_\alpha, X_\beta]$ for all unordered pairs (α, β) of different pairs of G_2 (the number of these pairs is 66).

It is easy to see that every vector $\alpha \in \mathfrak{h}^*$ is uniquely

written as $\alpha = ae_1 + be_2 + ce_3$, where $a + b + c = 0$, the isomorphism $\mathfrak{h}^* \approx \mathfrak{h}$ induced by the Euclidean structure introduced by us into $\mathfrak{h}^*$ sending that vector just to element (14) of the space $\mathfrak{h}$. Considering this we can denote element (14) also by α. An element α multiplied by $\frac{2}{|\alpha|^2}$ will be denoted by H_α. Thus $H_\alpha = \frac{2\alpha}{|\alpha|^2}$. In explicit form the element H_α is defined by the formula

$$H_\alpha = \frac{2}{a^2+b^2+c^2}(aE_{[3,\,2]} + bE_{[4,\,5]} + cE_{[7,\,6]}),$$

since it is easy to see that $|\alpha|^2 = a^2 + b^2 + c^2$.

Proposition 1. *For any vectors* α, $\beta \in G_2$ *we have*

(18) $[X_\alpha, X_{-\alpha}] = iH_\alpha$,

(19) $[X_\alpha, X_\beta] = 0$, *if* $\beta \neq -\alpha$ *and* $\alpha + \beta \notin G_2$, И

(20) $[X_\alpha, X_\beta] = N_{\alpha,\beta}X_{\alpha+\beta}$, *if* $\alpha + \beta \in G_2$ (*hence* $\beta \neq -\alpha$).

Here $N_{\alpha,\beta}$ *are some integers whose absolute values are subject to the formula*

(21) $$|N_{\alpha,\beta}| = p + 1,$$

where p *is the largest integer having the property that for every* $j = 0, 1, \ldots, p$ the vector $\beta - j\alpha$ *is in the configuration* G_2. □

The proof of this proposition will be obtained in Semester VI using a general theory. For the present all we can do is to suggest that the reader should honestly verify the proof by a calculation in all 66 cases.

Remark 3. That calculation will, of course, give us coefficients $N_{\alpha,\beta}$ with different signs (there will result in all 30 pairs (α, β) for which $N_{\alpha,\beta} \neq 0$). We could formulate a rule defining the signs, but for one thing, it is quite complicated and, for another, it has no invariant character. The thing is that relations (17), (18) together with the equation $\overline{X}_\alpha = X_{-\alpha}$ characterize elements X_α up to sign. In this sense the elements $\pm X_\alpha$ are given in $\mathfrak{g}_2^{\mathbb{C}}$ in an invariant way without any arbitrariness. The choice of signs which affect also the signs of coefficients $N_{\alpha,\beta}$, however, do not admit any invariant characterization.

With regard for this remark it can be said that Proposition 1 gives a complete definition of structural constants of the Lie algebra $\mathfrak{g}_2^{\mathbb{C}}$ (and hence of the Lie algebra $\mathfrak{g}_2$).

Algebras can be given by generators and relations as well as by structural constants.

Proposition 2. *The Lie algebra $\mathfrak{g}_2^{\mathbb{C}}$ can be given by four generators X_1, Y_1, X_2, Y_2 satisfying fifteen relations*

$$
\begin{aligned}
&[[X_1, Y_1], [X_2, Y_2]] = 0, \quad [X_1, Y_2] = 0, \quad [X_2, Y_1] = 0,\\
&[[X_1, Y_1], X_1] - 2X_1 = 0, \quad [[X_1, Y_1], X_2] + X_2 = 0,\\
&[[X_2, Y_2], X_1] + 3X_1 = 0, \quad [[X_2, Y_2], X_2] - 2X_2 = 0,\\
&[[X_1, Y_1], Y_1] + 2Y_1 = 0, \quad [[X_1, Y_1], Y_2] - Y_2 = 0,\\
(22)\quad &[[X_2, Y_2], Y_1] - 3Y_1 = 0, \quad [[X_2, Y_2], Y_2] + 2Y_2 = 0,\\
&[X_1 [X_1, X_2]] = 0, \quad [Y_1, [Y_1, Y_2]] = 0,\\
&[X_2, [X_2 [X_2 [X_2, X_1]]]] = 0, \quad [Y_2, [Y_2, [Y_2 [Y_2, Y_1]]]] = 0.
\end{aligned}
$$

Before giving a formal proof of Proposition 2 we discuss informally relations (22).

Assuming by definition $H_1 = -i[X_1, Y_1]$, $H_2 = -i[X_2, Y_2]$ and introducing numbers

$$n_{11} = n_{22} = 2, \qquad n_{12} = -1, \qquad n_{21} = -3,$$

we can rewrite relations (22) in the following form

$$
\begin{aligned}
&[H_p, H_q] = 0, \qquad [X_p, Y_q] = 0 \quad \text{if} \quad p \neq q,\\
(23)\quad &[H_p, X_q] = in_{p,q}X_q, \qquad [H_p, Y_q] = -in_{p,q}Y_q,\\
&(\operatorname{ad} X_p)^{|n_{pq}|+1} X_q = 0, \qquad (\operatorname{ad} Y_p)^{|n_{pq}|+1} Y_q = 0.
\end{aligned}
$$

It is in this form that we shall use them.

It can easily be seen that *relations* (23) *hold in* $\mathfrak{g}_2^{\mathbb{C}}$ *for* $X_1 = X_{f_1}$, $Y_1 = X_{-f_1}$, $X_2 = X_{e_2}$, $Y_2 = X_{-e_2}$ (*and* $H_1 = H_{-f_1}$, $H_2 = H_{e_2}$). Indeed, the first relation holds because, as was noticed above, the Lie bracket is zero for any elements in $\mathfrak{h}$. The second relation follows from formula (19) since $f_1 - e_2 = e_3 - 2e_2 \notin G_2$ and $e_2 - f_1 = 2e_2 - e_3 \notin G_2$. The third and fourth relations are special cases of formula (17)

since

$$\alpha(H_\beta) = \left(\alpha, \frac{2\beta}{|\beta|^2}\right) = \frac{2(\alpha, \beta)}{|\beta|^2}$$

$$= \begin{cases} 2, & \text{if } \alpha = \beta = f_1, e_2 \\ -3, & \text{if } \alpha = f_1, \quad \beta = e_2 \\ -1, & \text{if } \alpha = e_2, \quad \beta = f_1 \end{cases}$$

(we use the identification $\mathfrak{h} = \mathfrak{h}^*$ here) and the last two relations follow from formulas (19) and (20) of Proposition 1 since

$$\begin{aligned} &f_1 + e_2 = e_3 \in G_2, && \text{but } f_1 + e_3 \notin G_2, \\ (24)\quad &e_2 + f_1 = e_3 \in G_2, && e_2 + e_3 = -e_1 \in G_2, \\ &e_2 - e_1 = -f_3 \in G_2, && \text{but } e_2 - f_3 \notin G_2. \ \square \end{aligned}$$

If we consider a free Lie algebra $\mathfrak{l}$ with generators X_1, X_2, Y_1, Y_2 and its homomorphism φ into $\mathfrak{g}_2^{\mathbb{C}}$ defined by the formulas

$$\varphi(X_1) = X_{f_1}, \qquad \varphi(X_2) = X_{e_2},$$
$$\varphi(Y_1) = X_{-f_1}, \qquad \varphi(Y_2) = X_{-e_2},$$

then the statement proved will mean that the homomorphism φ nullifies the left-hand sides of all relations (22) and hence induces some homomorphism $\bar{\varphi}\colon \bar{\mathfrak{l}} \to \mathfrak{g}_2^{\mathbb{C}}$ into the Lie algebra $\mathfrak{g}_2^{\mathbb{C}}$ of the quotient algebra $\bar{\mathfrak{l}}$ of a Lie algebra $\mathfrak{l}$ mod the ideal generated by those left-hand sides. Proposition 2 is now equivalent to the statement that the *homomorphism* $\bar{\varphi}$ *is an isomorphism*. It is in this form that we shall prove it.

To avoid introducing unnecessary notation we permit ourselves to denote the elements of $\bar{\mathfrak{l}}$ by the same symbols as the corresponding elements of $\mathfrak{l}$. The symbol $X \sim Y$ means the proportionality of elements X and Y in $\bar{\mathfrak{l}}$ (i.e. they differ from each other by a numerical factor).

Consider in the algebra $\bar{\mathfrak{l}}$ the elements

$$\begin{aligned} & H_1 = [X_1, Y_1], && H_2 = [X_2, Y_2], \\ & X_1, X_2, X_3 = [X_2, X_1], && X_4 = [X_2, X_3], \\ (25)\quad & X_5 = [X_2, X_4], && X_6 = [X_4, X_3], \\ & Y_1, Y_2, Y_3 = [Y_2, Y_1], && Y_4 = [Y_2, Y_3], \\ & Y_5 = [Y_2, Y_4], && Y_6 = [Y_4, Y_3]. \end{aligned}$$

It turns out that *for any two elements U, V in the list* (25) *the element* $[U, V]$ *is either zero or proportional to some element in the same list*. Indeed, by hypothesis, $[H_1, H_2] = 0$, $[H_i, X_1] \sim X_1$, $[H_i, X_2] \sim X_2$, $i = 1, 2$. But if $[H, U] \sim U$ and $[H, V] \sim V$, then by the Jacobi identity

$$[H, [U, V]] = [[H, U], V] + [U, [H, V]] \sim [U, V].$$

Hence by induction

$$[H_p, X_q] \sim X_q$$

for any q. Similarly, it can be shown that

$$[H_p, Y_q] \sim Y_q.$$

Further, by hypothesis $[X_1, X_2] = X_3$ and $[X_1, X_3] = [X_1, [X_1, X_2]] = 0$. Therefore $[X_1, X_4] = [[X_1, X_2], X_3] + [X_2, [X_1, X_3]] = 0$, $[X_1, X_5] = [X_3, X_4] = -X_6$ and $[X_1, X_6] = 0$. Since $[X_1, Y_1] = H_1$, $[X_1, Y_2] = 0$, we have $[X_1, Y_3] = [[X_1, Y_2], Y_1] + [Y_2, [X_1, Y_1]] = -[[X_1, Y_1], Y_2] \sim [H_1, Y_2] \sim Y_2$ and hence $[X_1, Y_4] = -[[X_1, Y_3], Y_2] = 0$, $[X_1, Y_5] = 0$, $[X_1, Y_6] \sim [[X_1, Y_3], Y_4] \sim [Y_2, Y_4] = Y_5$. All the other brackets are calculated in exactly the same way. □

It follows from the statement proved that the span of elements (25) is a subalgebra of the Lie algebra $\bar{\mathfrak{l}}$ and hence, since it contains the generators X_1, X_2 and Y_1, Y_2, coincides with that algebra. In particular, this proves that $\dim \bar{\mathfrak{l}} \leqslant 14$. Now it is easy to prove Proposition 2.

Proof of Proposition 2. It is immediate from the above results (see, in particular, formulas (24)) that the homomorphism $\bar{\varphi}$ sends elements (25) to elements proportional, respectively, to the elements

(26) $$H_{f_1}, H_{e_1}, \quad X_{f_1}, X_{e_2}, X_{e_3}, X_{-e_1},$$
$$X_{-f_3}, X_{f_2}, X_{-f_1}, X_{-e_2}, X_{-e_2}, X_{e_1}, X_{f_3}, X_{-f_2}$$

(with regard to the elements X_6 and Y_6 this follows from the equation $e_3 - e_1 = f_2$). Since elements (26) constitute a basis of the algebra $\mathfrak{g}_2^{\mathbb{C}}$, it follows that the homomorphism $\bar{\varphi}_2$ is an epimorphism and hence, in view of the inequality $\dim \bar{\mathfrak{l}} \leqslant 14 = \dim \mathfrak{g}_2^{\mathbb{C}}$, also an isomorphism.

Thus we have studied the Lie algebra $\mathfrak{g}_2$ practically from all possible points of view.

Lecture 15

Identities in the octave algebra $\mathbb{C}\mathrm{a}$ · *Subalgebras of the octave algebra* $\mathbb{C}\mathrm{a}$ · *The Lie group* G_2 · *The triplicity principle for the group* Spin (8) · *The analogue of the triplicity principle for the group* Spin (9) · *The Albert algebra* $\mathbb{A}\mathrm{l}$ · *The octave projection plane*

With the Lie algebra $\mathfrak{g}_2$ studied, we can now turn to the corresponding Lie group $G_2 = \mathrm{Aut}\,\mathbb{C}\mathrm{a}$. The results of the preceding lecture characterize up to a covering the algebraic construction of the component of the identity of the group G_2. The main question, therefore, that remains to be discussed is that of determining whether G_2 is a connected group and, if so, what its fundamental group is.

To do this we must study in more detail the algebraic structure of the group $\mathbb{C}\mathrm{a}$.

Suppose first that $\mathcal{A}$ is an alternative algebra. Replacing in the identity of alternativity $(ab)\,b = a\,(bb)$ the element b by $x + y$, removing the parentheses and grouping similar terms we obtain the identity

$$ax \cdot y + ay \cdot x = a \cdot xy + a \cdot yx$$

(for simplicity we write dots instead of parentheses). This method of obtaining one identity from another is called *polarization* (or *linearization*).

Similarly, by polarizing the second identity of alternativity $b\,(ba) = (bb)\,a$ we obtain, with the variables rewritten, the identity

$$ax \cdot y + xa \cdot y = a \cdot xy + x \cdot ay.$$

The first identity implies that the expression $(ax)\,y - a\,(xy)$ (called the *associator* of the elements a, x, y) is skew-symmetric in x and y, and the second that the expression is skew-symmetric in a and x. Then it is skew-symmetric in a and y, which yields a third identity of alternativity,

$$ax \cdot y + yx \cdot a = a \cdot xy + y \cdot xa,$$

which, at $y = a$, assumes the form $(ax)\,a = a\,(xa)$ (this identity is also known as the *identity of elasticity*).

If the algebra $\mathcal{A}$, like $\mathbb{C}\mathrm{a}$, is in addition a metric algebra, then for any elements $a \in \mathcal{A}$ and $b = \lambda + b'$, where $\lambda \in \mathbb{R}$ and $b' \perp 1$, we have $(ab)\,(\lambda + b') = a \cdot b\,(\lambda + b')$, i.e. $ab \cdot b' = a \cdot bb'$. Hence $ab \cdot \lambda - ab \cdot b' = a \cdot b\lambda - a \cdot bb'$, i.e. $ab \cdot \bar{b} = a \cdot b\bar{b} = a\,(b,\ b)$. Polarizing this identity we obtain the identity

$$(1) \qquad ax \cdot \bar{y} + ay \cdot \bar{x} = 2\,(x,\ y)\,a,$$

a generalization of identity (2) of the preceding lecture (which results when $a = 1$).

Now let $\mathcal{A}$ be a normal algebra, i.e. let us have an identity $(ab,\ ab) = (a,\ a)\,(b,\ b)$ in it. Then by polarizing the identity first by $b = x + y$ and then by $a = u + v$ we obtain an identity

$$(2) \qquad (ux,\ vy) + (vx,\ uy) = 2\,(u,\ v)\,(x,\ y)$$

which holds for any elements u, v, x, y of a normed algebra $\mathcal{A}$ (and hence in particular of an algebra $\mathbb{C}\mathrm{a}$).

Of particular interest to us is the subset of the vector space $\mathbb{C}\mathrm{a}'$ consisting of elements ξ such that $|\,\xi\,| = 1$. That set is a 6-dimensional sphere. It will be denoted by S^6.

It can easily be seen that $\xi \in S^6$ *if and only if* $\xi^2 = -1$. Indeed, if $\xi \in \mathbb{C}\mathrm{a}'$, then $\bar{\xi} = -\xi$ and therefore $\xi^2 = -|\,\xi\,|^2$. Hence if $|\,\xi\,| = 1$, then $\xi^2 = -1$. Conversely if $\xi^2 = -1$, then $|\,\xi\,| = 1$ and hence $\xi\bar{\xi} = 1$, i.e. $\xi\,(-\bar{\xi}) = -1 = \xi\xi$. Hence $\bar{\xi} = -\xi$, i.e. $\xi \in \mathbb{C}\mathrm{a}'$, and since $|\,\xi\,| = 1$, we have $\xi \in S^6$. $\square$

It follows from linearity that $\xi \in \mathbb{C}\mathrm{a}'$ *if and only if* $\xi^2 = -|\,\xi\,|^2$.

Now let $\mathcal{H}$ be a unital (and therefore closed under conjugation) subalgebra of $\mathbb{C}\mathrm{a}$ other than $\mathbb{C}\mathrm{a}$ and let ζ be an

octave in S^6 orthogonal to $\mathscr{H}$. Then *for any element* $b \in \mathscr{H}$ *the octave* $b\zeta$ *is orthogonal to* $\mathscr{H}$. Indeed, assuming in (2) $u = 1$, $v = b$, $x = \zeta$ and $y = a$, where $a \in \mathscr{H}$, and considering that $(ab, \zeta) = 0$ (since $ab \in \mathscr{H}$) and $(\zeta, 1) = 0$ (by assumption) we at once see that $(b\zeta, a) = 0$ for any element $a \in \mathscr{H}$. $\square$

In particular, $b\zeta \perp 1$ (since $1 \in \mathscr{H}$), so that $\overline{b\zeta} = -b\zeta$. Besides, *for any elements* a, $b \in \mathscr{H}$,

$$a \cdot b\zeta = ba \cdot \zeta, \quad a\zeta \cdot b = a\bar{b} \cdot \zeta, \tag{3}$$

$$a\zeta \cdot b\zeta = -\bar{b}a.$$

Indeed, assuming in (1) $x = \zeta$, $y = \bar{b}$ and considering that $\zeta \perp b$ and hence $\zeta \perp \bar{b}$, we obtain an equation

$$a\zeta \cdot b + a\bar{b} \cdot \bar{\zeta} = 0,$$

equivalent to the second of identities (3). In a similar fashion, assuming in (1) $a = 1$, $x = a$, $y = \overline{b\zeta} = -b\zeta$, we get

$$-a \cdot b\zeta + b\zeta \cdot \bar{a} = -2\,(a, b\zeta) = 0,$$

and hence

$$a \cdot b\zeta = b\zeta \cdot \bar{a},$$

an equation equivalent to the first of identities (3) owing to the second identity already proved. Finally, with $b \in \mathbb{R}$, the third of identities (3) becomes $a\zeta \cdot b\zeta = -ba$ and hence reduces to the second identity. It suffices therefore to prove that identity only for $b \perp 1$. But in this case, by putting in (1) $x = \zeta$ and $y = \overline{b\zeta} = -b\zeta$ we get

$$a\zeta \cdot b\zeta + (a \cdot b\zeta)\,\zeta = -2\,(\zeta, b\zeta)\,a = 0,$$

since it follows, for $u = 1$, $v = b$, $x = y = \zeta$, from (2) that $(\zeta, b\zeta) = (1, b)\,(\zeta, \zeta) = 0$. Hence, by the identities already proved, $a\zeta \cdot b\zeta = -(ba)\,\zeta \cdot \zeta = ba = -\bar{b}a$. $\square$

Now it is easy to see that $\mathscr{H}$ *is an associative algebra*. Indeed, if $a, b, c \in \mathscr{H}$, then replacing in (1) a by $b\zeta$, x by c and y by $\bar{a}\zeta$ we obtain an identity

$$(b\zeta \cdot \bar{c}) \cdot \overline{\bar{a}\zeta} + (b\zeta \cdot \bar{a}\zeta)\,c = 2\,(\bar{c}, \bar{a}\zeta) \cdot b\zeta = 0$$

equivalent to the associative relation $(ab)c = a(bc)$ by virtue of identities (3). □

Now we are ready to prove our main lemma on automorphisms of an algebra $\mathbb{C}a$.

An automorphism $\Phi\colon \mathbb{C}a \to \mathbb{C}a$ sends elements i, j and e to elements $\xi = \Phi i$, $\eta = \Phi j$ while $\zeta = \Phi e$ in S^6 such that η is orthogonal to ξ and ζ is orthogonal to ξ, η and $\xi\eta$. It turns out that the latter conditions are not only necessary but also sufficient for the existence of the automorphism Φ:

Lemma 1. *For any elements* ξ, η, $\zeta \in S^6$ *such that:*

(a) η *is orthogonal to* ξ;

(b) ζ *is orthogonal to* ξ, η *and* $\xi\eta$ *there is an automorphism* Φ *(obviously unique) of an algebra* $\mathbb{C}a$ *for which*

$$\xi = \Phi i, \qquad \eta = \Phi j, \qquad \zeta = \Phi e.$$

Proof. Since $\xi \in S^6$ and $\eta \in S^6$, we have $\xi^2 = -1$ and $\eta^2 = -1$, and since $\xi \perp \eta$, we have $\xi\eta = -\eta\xi$. Therefore $\overline{\xi\eta} = \bar{\eta}\bar{\xi} = \eta\xi = -\xi\eta$ and hence $\xi\eta \in S^6$ (since $|\xi\eta| = |\xi|\cdot|\eta| = 1$). Consequently $(\xi\eta)^2 = -1$. Besides, by alternativity $\xi(\xi\eta) = -\eta$ and $(\xi\eta)\eta = -\xi$ and, by putting in (28) $u = \imath = \xi$, $x = \eta$ and $y = 1$, we get $(\xi\eta, \xi) = (\xi, \xi)(\eta, 1) = 0$, from which it follows that $(\xi\eta)\xi = -\xi(\xi\eta) = \eta$. Since similarly $\eta(\xi\eta) = \xi$, we see that multiplying any number of the elements ξ and η in any order we shall obtain only elements ± 1, $\pm\xi$, $\pm\eta$ and $\pm\xi\eta$. This means that elements of the form

$$a + b\xi + c\eta + d\xi\eta,\ a,\ b,\ c,\ d \in \mathbb{R},$$

constitute a subalgebra $\mathscr{H}$ of $\mathbb{C}a$ which is of dimension 4 and hence, according to the foregoing, is an associative algebra. Then it can be easily seen that the correspondences $1 \mapsto 1$, $i \mapsto \xi$, $j \mapsto \eta$, $k \mapsto \xi\eta$ define an isomorphism of the algebra of quaternions $\mathbb{H}$ onto the algebra $\mathscr{H}$.

Further, the element ζ orthogonal by hypothesis to elements 1, ξ, η and $\xi\eta$ is orthogonal to the entire algebra $\mathscr{H}$. Therefore there are identities (3) holding for it. Comparing identities (3) with formulas (1) we immediately discover that the isomorphism $\mathbb{H} \to \mathscr{H}$ we have constructed can be extended to a homomorphism (in which $e \mapsto \zeta$) of an algebra $\mathbb{C}a$ onto a subalgebra generated by the subalgebra $\mathbb{H}$ and the element ζ. Since any nonzero homomorphism of a unital

division algebra is necessarily a monomorphism (if $\xi \neq 0$ goes into zero where does ξ^{-1} go?) and since any monomorphic mapping of a finite-dimensional algebra into itself is necessarily an automorphism (for an injective linear operator acting in a finite-dimensional space is bijective), it follows that we have constructed an automorphism $\mathbb{C}a \to \mathbb{C}a$ sending elements i, j, e to elements ξ, η, ζ.

This completes the proof of Lemma 1. □

From Lemma 1 it follows, in particular, that the *group* $G_2 = \operatorname{Aut} \mathbb{C}a$ *acts transitively on* S^6, i.e. that the mapping $G_2 \to S^6$ defined by the formula $\Phi \mapsto \Phi i$ is surjective. This means that the sphere S^6 is diffeomorphic to the quotient manifold G_2/K of the group G_2 mod the subgroup K consisting of all automorphisms leaving the element i fixed:

$$G_2/K \approx S^6.$$

For any automorphism $\Phi \in K$ the element $\eta = \Phi j$ in S^2 is orthogonal to an element i and hence is in some five-dimensional sphere S^5 (in the equator of the sphere S^6 with pole i). By Lemma 1, the mapping $\Phi \mapsto \Phi j$ of the group K onto S^5 is surjective. Hence

$$K/L \approx S^5,$$

where L is a subgroup of K consisting of automorphisms leaving the element j fixed.

For automorphisms Φ in L the element $\zeta = \Phi e$ in S^6 is orthogonal to elements i, j, k, i.e. it is in some three-dimensional sphere $S^3 \subset S^6$. By th same Lemma 1, the mapping $\Phi \mapsto \Phi e$ is a diffeomorphism of the group L onto the sphere S^3:

$$L \approx S^3.$$

In topological terms this means that the group G_2 stratifies over S^6 into manifolds diffeomorphic to K which in turn stratify over a sphere S^5 into three-dimensional spheres S^3.

Proposition 1. *The group G_2 is connected and simply connected. Every Lie group locally isomorphic t G_2 is isomorphic to it.*

Proof. The first statement is immediate from th obtained results by virtue of Lemma 2, Lecture 1, the corollary to

Lemma 1 of Lecture 9 and Proposition 7 of Lecture 12. The second statement means that G_2 has no nontrivial discrete invariant subgroups. Since (Lemma 6 of Lecture 9) all discrete invariant subgroups of a connected Lie group are contained in its centre, to prove the statement it suffices to establish that the centre of G_2 is trivial, i.e. that the automorphism Φ_0 of an algebra $\mathbb{C}a$ commutative with each of its automorphisms Φ is necessarily an identity automorphism. If Φ_0 is commutative with Φ and if $\Phi \in K$, i.e. $\Phi i = i$, then $\Phi(\Phi_0 i) = \Phi_0 i$. It is, however, immediate from Lemma 1 that the last equation is possible for all elements of the group K only when $\Phi_0 i = i$. In a similar fashion it can be proved that $\Phi_0 j = j$. Hence $\Phi_0 = \mathrm{id}$. □

In view of the simple connectedness of the Lie group G_2 its algebraic structure is completely determined by the algebraic structure of $\mathfrak{g}_2$ studied above.

Remark 1. As already noted in Lecture 14, the subspace $\mathscr{V}$ of the algebra $\mathbb{C}a$ orthogonal to the elements 1 and i is a vector space over the field $\mathbb{C}$ with a basis j, e, g. The scalar product in $\mathbb{C}a$ defines in $\mathscr{V}$ a Hermitian scalar product with respect to which the basis j, e, g is orthonormal. Any automorphism Φ: $\mathbb{C}a \to \mathbb{C}a$ which leaves i fixed, i.e. which is in the subgroup K, defines an operator $\mathscr{V} \to \mathscr{V}$ linear over $\mathbb{C}$. This operator preserves the scalar product, i.e. it is a unitary operator. Since its determinant is readily seen to be equal to unity, the group K is thus identified with some subgroup of the group SU (3). It is immediate from Lemma 1 that in fact the group K coincides with the entire group SU (3). Thus it may be assumed that SU (3) $\subset G_2$, with G_2/SU (3) $\approx S^6$. The Lie group $\mathfrak{k}$ of the group K consists of differentiations D for which $Di = 0$. This proves anew that these differentiations constitute a Lie algebra isomorphic to the Lie algebra $\mathfrak{su}$ (3).

An algebra $\mathbb{C}a$ can be used to study the group SO (8) as well, since every element of SO (8) may be assumed to be an orthogonal operator $\mathbb{C}a \to \mathbb{C}a$. Here it is more convenient, however, to go from the group SO (8) to its universal covering group Spin (8).

The results to be presented below concerning the groups Spin (8) and Spin (9) are due to Jacobson.

Ignoring in $\mathbb{C}a$ multiplication, i.e. considering $\mathbb{C}a$ simply as a Euclidean space we can construct Clifford algebras $\mathbb{C}l_+(\mathbb{C}a)$ and $\mathbb{C}l(\mathbb{C}a')$. Thus elements $i, j, k, e, f = ie, g = je, h = ke$ will now be generators of $\mathbb{C}l(\mathbb{C}a')$. In this capacity we shall denote them, following Lecture 13, by $e_1, \ldots, e_7$. In $\mathbb{C}l_+(\mathbb{C}a)$ we add to these generators yet another one, the identity element of the algebra $\mathbb{C}a$. Deviating somewhat from the notation adopted in Lecture 13 we shall denote that additional generator by e_0.

According to the remark to Proposition 8 of Lecture 13 the algebra $\mathbb{C}l(\mathbb{C}a')$ is isomorphic to $\mathbb{C}l_+^0(\mathbb{C}a)$, with the role of e_n in the isomorphism of that remark now being played by e_0, of course. Thus the isomorphism will be defined by the formula

$$\omega_+(e_I) = \begin{cases} \bar{e}_I, & \text{if } |I| \text{ is even} \\ e_0\bar{e}_I, & \text{if } |I| \text{ is odd,} \end{cases}$$

where I is a subset of the set $\{1, \ldots, 7\}$.

The vector space $\mathbb{C}a$ is, by definition, embedded into the algebra $\mathbb{C}l_+(\mathbb{C}a)$. We shall assume it to be embedded into $\mathbb{C}l(\mathbb{C}a')$ as well by identifying for this purpose its identity element with the identity 1 of $\mathbb{C}l(\mathbb{C}a')$. It is easy to see that by this identification, for every element of $\mathbb{C}l_+^0(\mathbb{C}a)$ of the form e_0u, where $u \in \mathbb{C}a$,

$$\omega_+^{-1}(e_0u) = u.$$

Indeed, if $u = \lambda e_0 + u'$, where $\lambda \in \mathbb{R}$ and $u' \in \mathbb{C}a'$, then $e_0u = \lambda + e_0u'$ and therefore $\omega_+^{-1}(e_0u) = \lambda + \bar{u}' = \lambda + u' = u$ (conjugation is regarded here as conjugation in $\mathbb{C}l_+(\mathbb{C}a)$ rather than in $\mathbb{C}a$, so $\bar{u}' = u'$). $\square$

In view of the alternativity of $\mathbb{C}a$, for any elements $x \in \mathbb{C}a$ and $u \in \mathbb{C}a'$,

$$(xu)u = x \cdot u^2 = -|u|^2 x$$

(recall that $u^2 = -|u|^2$ if $u \in \mathbb{C}a'$), which implies that for a linear operator $R_u\colon x \mapsto xu$, $u \in \mathbb{C}a'$, we have

$$R_u^2 = -|u|^2 E,$$

Therefore the correspondence $u \mapsto R_u$ is extended to some homomorphism

$$R\colon \mathrm{Cl}\,(\mathbb{C}\mathrm{a}') \to \mathrm{End}\,\mathbb{C}\mathrm{a},$$

where End $\mathbb{C}$a is the algebra of all linear operators $\mathbb{C}\mathrm{a} \to \mathbb{C}\mathrm{a}$.

Since for any element $u = \lambda + u' \in \mathbb{C}\mathrm{a} \subset \mathrm{Cl}\,(\mathbb{C}\mathrm{a}')$ we have $R\,(\lambda + u') = \lambda E + R_{u'} = R_{\lambda+u'}$, the homomorphism R is an extension of $u \mapsto R_u$ for any $u \in \mathbb{C}\mathrm{a}$ as well.

In a similar fashion we can prove the existence of such a homomorphism

$$L\colon \mathrm{Cl}\,(\mathbb{C}\mathrm{a}') \to \mathrm{End}\,\mathbb{C}\mathrm{a},$$

$L_u = L_u\colon X \to ux$ for any element $u \in \mathbb{C}\mathrm{a}$.

Since the algebra $\mathrm{Cl}\,(\mathbb{C}\mathrm{a})$ is identified with $\mathrm{Cl}_+\,(8)$ and the algebra End $\mathbb{C}$a with the algebra $\mathbb{R}(8)$, this gives rise to two composition homomorphisms

$$\text{(4)}\qquad \mathrm{Spin}_+\,(8) \in \mathrm{Cl}^0_+\,(8) = \mathrm{Cl}^0_+\,(\mathbb{C}\mathrm{a}) \xrightarrow{\omega_+^{-1}} \mathrm{Cl}\,(\mathbb{C}\mathrm{a}') \overset{R,\,L}{\rightrightarrows} \mathrm{End}\,\mathbb{C}\mathrm{a} = \mathbb{R}\,(8).$$

Since $\omega_+^{-1}\,(e_0u) = u$, associated with every element of Spin (8) of the form e_0u, where $u \in S^7 \subset \mathbb{C}\mathrm{a}$, is the operator $\mathbb{R}_u\colon \mathbb{C}\mathrm{a} \to \mathbb{C}\mathrm{a}$ for one of these homomorphisms and the operator $L_u\colon \mathbb{C}\mathrm{a} \to \mathbb{C}\mathrm{a}$ for the other. Since $|\,u\,| = 1$ and $\mathbb{C}$a is normed, these operators are orthogonal. As elements of the form e_0u, $u \in S^7$, generate the group $\mathrm{Spin}_+\,(8)$, this proves that homomorphisms (4) map the group $\mathrm{Spin}_+\,(8)$ into SO (8) (or, without making the last identification, into the group Ort $\mathbb{C}$a of orthogonal operators $\mathbb{C}\mathrm{a} \to \mathbb{C}\mathrm{a}$).

Elements of SO (8) (or Ort $\mathbb{C}$a) which are the images of an element $a \in \mathrm{Spin}_+\,(8)$ under homomorphisms (4) will be denoted by a^R and a^L, respectively.

According to the above calculations, if $a = (e_0u_1)\ldots(e_0u_r)$, where $u_1, \ldots, u_r \in S^7$, then

$$a^R = R_{u_1} \circ \ldots \circ R_{u_r} \quad\text{and}\quad a^L = L_{u_1} \circ \ldots \circ L_{u_r}.$$

Remark 2. It follows immediately from the general theory of matrix representations of groups Spin (n) that homomorphisms $a \mapsto a^R$ and $a \to a^L$ are equivalent to semispinor representations of the group Spin $(8) \approx \mathrm{Spin}_+\,(8)$ (see formula (20) of Lecture 13 for $m = 1$) which, we notice,

having a discrete kernel, are in this case coverings (obviously, double ones). However, this equivalence is easy to prove directly as well (one should only keep in mind that exactly representations (20) of Lecture 13 will result if for the identification $\mathbb{C}l^0_+(8) = \mathbb{C}l^0_+(\mathbb{C}a)$ one takes as basis elements of $\mathbb{C}a$ the elements $1, e, h, g, i, f, -j, k$ and for the identification $\operatorname{End}\mathbb{C}a = \mathbb{R}(8)$ one takes the elements $-1, i, -j, -k, e, f, g, h$). We shall not need this equivalence and therefore shall not prove it.

Besides homomorphisms $a \mapsto a^R$ and $a \mapsto a^L$ we also have the homomorphism φ_0: $\mathrm{Spin}_+(8) \to SO(8)$ in Proposition 4 of Lecture 13 which associates every element $a \in \mathrm{Spin}_+(8)$ with an orthogonal operator $\varphi_0(a)$: $x \mapsto ax\bar{a}$ acting in the vector space $\mathbb{C}a$. This operator will now be denoted by a^T. Since $\operatorname{Ker}\varphi_0 = \{1, -1\}$, we have $(-a)^T = a^T$ and, in particular, $(e_0u)^T = (ue_0)^T$. On the other hand, $(ue_0)^T = u^\perp e_0^\perp$, with $u^\perp$ a symmetry with respect to the hyperplane perpendicular to a vector u (see proof of Proposition 4 in Lecture 13). But by formula (2) of the preceding lecture, for any octaves $x, u \in \mathbb{C}a$ we have $uxu = \bar{\bar{u}}xu = (2(u, \bar{x}) - \bar{x}\bar{u})u$ (conjugation in $\mathbb{C}a$) from which it follows at $|u| = 1$ that $uxu = -u^\perp(\bar{x})$, i.e. that $uxu = u^\perp e_0^\perp(x)$ since $e_0^\perp x = -\bar{x}$. Introducing an operator T_u: $x \mapsto uxu$, i.e. an operator $T_u = R_u \circ L_u = L_u \circ R_u$, we thus obtain $T_u = u^\perp e_0^\perp$ and hence $T_u = (ue_0)^T = (e_0u)^T$. Therefore if $a = (e_0u_1)\ldots(e_0u_r)$, then

$$a^T = T_{u_1} \circ \ldots \circ T_{u_r}$$

as well as for the operators a^R and a^L.

Lemma 2 (central Moufang identity). *In every alternative algebra there is an identity*

$$u \cdot xy \cdot u = ux \cdot yu. \tag{5}$$

Proof. In view of the identities of alternativity and elasticity there is an identity

$$y^2x \cdot y = (y \cdot yx)\, y = y\,(yx \cdot y) = y\,(y \cdot xy) = y^2 \cdot xy$$

and hence, in view of the skew-symmetry of the associators, an identity

$$xy^2 \cdot y = x \cdot y^3,$$

i.e. an identity

$$x \cdot y^3 = (xy \cdot y)\, y.$$

Polarizing this identity by y, i.e. putting $y = a + b$ and grouping similar terms, we obtain an identity

$$x \cdot a^2 b + x \cdot ba^2 + x \cdot aba + x \cdot bab + x \cdot ab^2 + x \cdot b^2 a$$
$$= xa^2 \cdot b + xb \cdot a^2 + (xa \cdot b)\, a + (xb \cdot a)\, b + xa \cdot b^2 + xb^2 \cdot a.$$

By the skew-symmetry of the associators, the sums of the two first terms in each row are equal. For the same reason so are the sums of the last two terms. Therefore

$$x \cdot aba + x \cdot bab = (xa \cdot b)\, a + (xb \cdot a)\, b.$$

Replacing b by λb, where $\lambda \in \mathbb{R}$, reducing by λ and putting $\lambda = 0$ we obtain an identity

$$x \cdot aba = (xa \cdot b)\, a$$

called the *right Moufang identity*.

By this identity and the skew-symmetry of the associators,

$$\begin{aligned} ab \cdot xa - a \cdot bx \cdot a &= ab \cdot xa - (ab \cdot x)\, a + (ab \cdot x - a \cdot bx)\, a \\ &= (x \cdot ab)\, a - x \cdot aba + (xa \cdot b - x \cdot ab)\, a \\ &= (xa \cdot b)\, a - x \cdot aba = 0, \end{aligned}$$

which differ only in notation from identity (5). □

Lemma 2 implies that

$$T_u\,(xy) = L_u x \cdot R_u y,$$

from which by virtue of the formulas for a^R, a^L and a^T, proved above, we get by induction

$$a^T\,(xy) = a^L x \cdot a^R y$$

for any octaves $x, y \in \mathbb{C}\mathrm{a}$ and any element $a \in \mathrm{Spin}_+\,(8)$.

Now we can go from the group $\mathrm{Spin}_+\,(8)$ to the group $\mathrm{Spin}\,(8)$ isomorphic to it. Denoting by a_+ an element in $\mathrm{Spin}_+\,(8)$ corresponding to any element a in $\mathrm{Spin}\,(8)$ and putting $a^K = a_+^K$, where $K = T, L, R$, we obtain the following proposition:

Proposition 2. *For an element* $a \in \mathrm{Spin}\,(8)$ *there is an identity*

$$a^T\,(xy) = a^L x \cdot a^R y, \qquad x, y \in \mathbb{C}\mathrm{a}.$$

This proposition is called the *triplicity principle for the group* Spin (8).

Remark 3. As we know, the homomorphism $a \mapsto a^T$ is a covering, and according to Remark 1 so are the homomorphisms $a \mapsto a^L$ and $a \mapsto a^R$. For any $K = T, L, R$ therefore the homomorphism $a \mapsto a^K$ induces an isomorphism of the Lie algebra $\mathfrak{l}$ (Spin (8)) onto $\mathfrak{l}$ (SO (8)) $= \mathfrak{so}$ (8). Identifying these Lie algebras by means of the first one of these isomorphisms we obtain from the remaining two some automorphisms of the Lie algebra $\mathfrak{so}$ (8). Denoting by A^λ and A^ρ images of a matrix $A \in \mathfrak{so}$ (8) under those automorphisms we have, as can be easily seen, an identity

$$(6) \quad A^\lambda x \cdot y + x \cdot A^\rho y = A\,(xy), \quad x, y \in \mathbb{C}\mathrm{a},\ A \in \mathfrak{so}\,(8).$$

This is called the *infinitesimal principle of triplicity.* Its direct proof is available in [11].

The following proposition can be regarded as the converse of the triplicity principle.

Proposition 3. *If orthogonal operators* A, B, C: $\mathbb{C}\mathrm{a} \to \mathbb{C}\mathrm{a}$ *have the property that*

$$A\,(xy) = Bx \cdot Cy$$

for any octaves $x, y \in \mathbb{C}\mathrm{a}$, *then those operators are necessarily unimodular* (*i.e. they are* in SO (8)) *and there is one and only one element* $a \in$ Spin (8) *for which*

$$(7) \qquad A = a^T, \qquad B = a^L, \qquad C = a^R.$$

Proof. If $A \in$ SO (8) and so there is an element $a \in$ Spin (8) such that $A = a^T$, then $xy = B'x \cdot C'y$, where $B' = (a^L)^{-1} \circ B$ and $C' = (a^R)^{-1} \circ C$. Then $B'x = xb$, with $b = (C'1)^{-1}$, and $C'y = cy$, with $c = (B'1)^{-1}$, and hence

$$xy = xb \cdot cy.$$

Setting here $x = y = 1$, we get $bc = 1$, and replacing x by $xc = xb^{-1}$ we get $xc \cdot y = x \cdot cy$. It is easy to see (taking as x and y all possible basis elements of the vector space $\mathbb{C}\mathrm{a}'$) that, with x and y arbitrary, that equation is possible only when $c \in \mathbb{R}$, i.e., the operator C' being orthogonal, when $c = \pm 1$. If $c = 1$, then the element a satisfies relations (7), and if $c = -1$, then it should be replaced by $-a$. The

uniqueness of this element is obvious (for if $a^T = b^T$, then $a = \pm b$ and therefore $a^L = \pm b^L$).

Notice that the operators B and C have turned out to be in the group SO (8). To complete the proof therefore it only remains to be shown that the inclusion $A \in \mathrm{O}(8) \setminus \mathrm{SO}(8)$ is impossible. Without loss of generality we may clearly assume that $A: x \to \bar{x}$, i.e. that $Bx \cdot Cy = \overline{xy}$. Then $Bx = \bar{x}b$, with $b = (C1)^{-1}$, and $Cy = c\bar{y}$, with $c = (B1)^{-1}$, i.e. $\bar{x}b \cdot c\bar{y} = \overline{xy}$ and hence (with x replaced by $\bar{x}$ and y by $\bar{y}$)

$$xb \cdot cy = yx.$$

It follows for $x = y = 1$ that $bc = 1$ and hence $x \cdot cy = y \cdot xc$. In particular, $cy = yc$ for all $y \in \mathbb{C}\mathrm{a}$, which is possible only when $c \in \mathbb{R}$. Therefore $xy = yx$, which is absurd. Hence the case $A \in \mathrm{O}(8) \setminus \mathrm{SO}(8)$ is impossible. $\square$

Remark 4. A similar converse is possible for the infinitesimal principle of triplicity (6) as well: *if A, B, C are skew-symmetric operators $\mathbb{C}\mathrm{a} \to \mathbb{C}\mathrm{a}$ such that*

$$A(xy) = Bx \cdot y + x \cdot Cy \quad \textit{for any} \quad x, y \in \mathbb{C}\mathrm{a},$$

then $B = A^\lambda$ and $C = A^\rho$. Indeed, for the operators $B' = B - A^\lambda$ and $C' = C - A^\rho$ there is an identity $B'x \cdot y = -x \cdot C'y$, from which it follows that $B'x = xb$, with $b = -C'1$, and $C'y = cy$, with $y = -B'1$. Thus $xb \cdot y = -x \cdot cy$, from which it follows for $x = y = 1$ that $b = -c$ and hence $xb \cdot y = x \cdot by$. Therefore $b \in \mathbb{R}$, i.e. the operator B' is diagonal. Hence, by virtue of skew-symmetry, $B' = 0$ and therefore $C' = 0$. $\square$

The analogue of the triplicity principle holds for the group Spin (9) as well. To obtain it we introduce vector spaces $\mathbb{C}\mathrm{a}^\oplus = \mathbb{R} \oplus \mathbb{C}\mathrm{a}$ and $\mathbb{C}\mathrm{a}^2 = \mathbb{C}\mathrm{a} \oplus \mathbb{C}\mathrm{a}$. To avoid confusion with a scalar product the elements of the vector space $\mathbb{C}\mathrm{a}^2$ will be denoted by $\{\xi, \eta\}$, where $\xi, \eta \in \mathbb{C}\mathrm{a}$, and accordingly the elements of $\mathbb{C}\mathrm{a}^\oplus$ will be denoted by $\{r, \rho\}$, where $r \in \mathbb{R}$, $\rho \in \mathbb{C}\mathrm{a}$.

We associate every element $x = \{\xi, \eta\}$ of $\mathbb{C}\mathrm{a}^2$ and every element $u = \{r, \rho\}$ of $\mathbb{C}\mathrm{a}^\oplus$ with an element xu of $\mathbb{C}\mathrm{a}^2$ defined by the formula

$$xu = \{-r\xi + \overline{\rho\eta}, r\eta + \overline{\xi\rho}\}.$$

Clearly, this multiplication is bilinear (over $\mathbb{R}$) and has the property that if $xu = xv$ for all $x \in \mathbb{C}a^2$, then $u = v$ (if $-r\xi + \overline{\overline{\rho\eta}} = -s\xi + \overline{\overline{\sigma\eta}}$ for all ξ and η, then $-r\xi = -s\xi$ and therefore $r = s$ and $\overline{\overline{\rho\eta}} = \overline{\overline{\sigma\eta}}$ and therefore $\rho = \sigma$).

Lemma 3. *For any elements $x \in \mathbb{C}a^2$ and u, $v \in \mathbb{C}a^{\oplus}$ there is an identity*

$$xu\cdot v = -xv\cdot v^{\perp}u, \tag{8}$$

where $v^{\perp}$ is as ever a symmetry in the hyperplane perpendicular to the vector v.

Proof. Let $u = \{r, \rho\}$, $v = \{s, \sigma\}$. Clearly, it may be assumed without loss of generality that u and v are unit vectors, i.e. vectors satisfying the relations $r^2 + |\rho|^2 = 1$, $s^2 + |\sigma|^2 = 1$. Then $v^{\perp}u = \{r - 2(u, v)s, \rho - 2(u, v)\sigma\}$, where $2(u, v) = 2rs + \bar{\rho}\sigma + \bar{\sigma}\rho$.

By virtue of its linearity it suffices to prove identity (8) only for $x = \{\xi, 0\}$ and $x = \{0, \eta\}$. But if $x = \{\xi, 0\}$, then

$$xu = \{-r\xi, \overline{\bar{\xi}\rho}\}, \qquad xv = \{-s\xi, \overline{\bar{\xi}\sigma}\},$$
$$xu\cdot v = \{rs\xi + \bar{\sigma}\cdot\rho\xi, s\bar{\xi}\bar{\rho} - r\bar{\xi}\bar{\sigma}\}$$

and

$$\begin{aligned} xv\cdot v^{\perp}u &= \{(r - 2(u, v)s)s\xi \\ &\quad + \overline{(\rho - 2(u, v)\sigma)}\cdot\sigma\xi, (r - 2(u, v)s)\bar{\xi}\bar{\sigma} \\ &\quad - s\bar{\xi}\overline{(\rho - 2(u, v)\sigma)}\} \\ &= \{rs\xi - 2(u, v)s^2\xi + \bar{\rho}\cdot\sigma\xi - 2(u, v)\bar{\sigma}\sigma\xi, r\bar{\xi}\bar{\sigma} \\ &\quad - 2(u, v)s\bar{\xi}\bar{\sigma} - s\bar{\xi}\bar{\rho} + 2(u, v)s\bar{\xi}\bar{\sigma}\} \\ &= \{[rs - 2(u, v)(s^2 + |\sigma|^2)]\xi + \bar{\rho}\cdot\sigma\xi, r\bar{\xi}\bar{\sigma} - s\bar{\xi}\bar{\rho}\}, \end{aligned}$$

and hence (since $rs - 2(u, v)(s^2 + |\sigma|^2) = rs - 2(u, v) = -rs - \bar{\rho}\sigma - \bar{\sigma}\rho$)

$$xu\cdot v + xv\cdot v^{\perp}u = \{\bar{\sigma}\cdot\rho\xi - \bar{\sigma}\rho\cdot\xi + \bar{\rho}\sigma\cdot\xi - \bar{\rho}\cdot\sigma\xi, 0\},$$

which is equal to $\{0, 0\}$ by virtue of the skew-symmetry of the associators and because of the obvious fact that when one of the elements is replaced by its conjugate the associator changes sign.

The case $x = \{0, \eta\}$ is considered in a similar way. $\square$

Now associate every element $u \in \mathrm{Ca}^{\oplus}$ with a linear operator R_u: $x \mapsto xu$ acting in the space Ca^2. Since, as can be shown by a direct calculation, $xu \cdot u = |u^2|\, x$ for any elements $x \in \mathrm{Ca}^2$, $u \in \mathrm{Ca}^{\oplus}$, i.e. $R_u^2 = |u^2|\, E$, the linear mapping $u \mapsto R_u$ of the space $\mathrm{Ca}^{\oplus}$ into the algebra of linear operators $\mathrm{End}\,\mathrm{Ca}^2$ can be extended uniquely to some homomorphism of algebras

$$R\colon \mathrm{Cl}_+ (\mathrm{Ca}^{\oplus}) \to \mathrm{End}\,\mathrm{Ca}^2.$$

Since the algebras $\mathrm{Cl}_+ (\mathrm{Ca}^{\oplus})$ and $\mathrm{End}\,\mathrm{Ca}^2$ can be identified with $\mathrm{Cl}_+ (9)$ and $\mathbb{R}(16)$, respectively, there arises a composition homomorphism

$$\text{(9)}\quad \mathrm{Spin}_+ (9) \subset \mathrm{Cl}_+ (9) = \mathrm{Cl}\,(\mathrm{Ca}^{\oplus}) \xrightarrow{R} \mathrm{End}\,\mathrm{Ca}^2 = \mathbb{R}(16).$$

If $u = \{r, \rho\} \in S^8 \subset \mathrm{Ca}^{\oplus}$, i.e. $r^2 + |\rho|^2 = 1$ and $x = |\xi, \eta| \in \mathrm{Ca}^2$, then

$$\begin{aligned} |xu|^2 &= |\{-r\xi + \bar{\rho}\bar{\eta},\ r\eta + \bar{\xi}\bar{\rho}\}|^2 \\ &= (-r\xi + \bar{\rho}\bar{\eta})(-r\bar{\xi} + \eta\rho) + (r\eta + \bar{\xi}\bar{\rho})(r\bar{\eta} + \rho\xi) \\ &= r^2\xi\bar{\xi} - r\xi\cdot\eta\rho - r\bar{\rho}\bar{\eta}\cdot\bar{\xi} + \bar{\rho}\bar{\eta}\cdot\eta\rho \\ &\quad + r^2\eta\bar{\eta} + r\eta\cdot\rho\xi + r\bar{\xi}\bar{\rho}\cdot\bar{\eta} + \bar{\xi}\bar{\rho}\cdot\rho\xi \\ &= (r^2 + |\rho|^2)(|\xi|^2 + |\eta|^2) + rz = |x|^2 + rz, \end{aligned}$$

where

$$z = -\xi\cdot\eta\rho - \bar{\rho}\bar{\eta}\cdot\bar{\xi} + \eta\cdot\rho\xi + \bar{\xi}\bar{\rho}\cdot\bar{\eta}.$$

But putting $[\xi, \eta] = \xi\eta - \eta\xi$ and $(\xi, \eta, \zeta) = \xi\eta\cdot\zeta - \xi\cdot\eta\zeta$, is easily seen to yield

$$z = [\eta\rho, \xi] - (\eta, \rho, \xi) + [\bar{\xi}, \bar{\rho}\bar{\eta}] + (\bar{\xi}, \bar{\rho}, \bar{\eta}).$$

As was noted earlier, when any element is replaced by its conjugate the associator (ξ, η, ζ) changes sign. Therefore $(\bar{\xi}, \bar{\rho}, \bar{\eta}) = -(\xi, \rho, \eta)$. Similarly $[\bar{\xi}, \bar{\rho}\bar{\eta}] = [\bar{\xi}, \overline{\eta\rho}] = [\xi, \eta\rho]$. Therefore

$$z = [\eta\rho, \xi] + [\xi, \eta\rho] - (\eta, \rho, \xi) - (\xi, \rho, \eta) = 0$$

due to the skew-symmetry of the associators. Thus $|xu|^2 = |x|^2$. This means that the linear operator $R_u = Ru$ is orthogonal, from which it follows immediately that homomorphism (9) sends the group $\mathrm{Spin}_+(9)$ (even $\mathrm{pin}_+(9)$) to $SO(9)$.

The image of an element $a \in \mathrm{Spin}_+(9)$ in $SO(9)$ under the homomorphism (9), interpreted as an orthogonal operator in the space $\mathbb{C}\mathrm{a}^2$, will be denoted by a^R.

Remark 5. The homomorphism $a \mapsto a^R$ is a spinor representation of the group $\mathrm{Spin}_+(9) \approx \mathrm{Spin}(9)$, but we shall not need this fact and shall not prove it.

The image of an element $a \in \mathrm{Spin}_+(9)$ under the homomorphism φ_0: $\mathrm{Spin}_+(9) \to SO(9)$ in Proposition 4 of Lecture 13, interpreted as an orthogonal operator in the space $\mathbb{C}\mathrm{a}^{\oplus}$, will be denoted by a^T.

Besides, as above, for any element $a \in \mathrm{Spin}(9)$ we set $a^R = a_+^R$ and $a^T = a_+^T$, where a_+ is an element of $\mathrm{Spin}_+(9)$ corresponding to the element a under the isomorphism $\mathrm{Spin}(9) \approx \mathrm{Spin}_+(9)$. Then the following proposition holds:

Proposition 4. *For an element* $a \in \mathrm{Spin}(9)$ *there is an identity*

$$(10) \qquad a^R(xu) = a^R x \cdot a^T u, \qquad x \in \mathbb{C}\mathrm{a}^2, \qquad u \in \mathbb{C}\mathrm{a}^{\oplus}.$$

Proof. Since the group $\mathrm{Spin}(9)$ is generated by elements of the form vw, where $v, w \in S^8 \subset \mathbb{C}\mathrm{a}^{\oplus}$, it suffices to prove identity (10) only for $a = vw$. But by Lemma 2 and the definition of the homomorphism R

$$\begin{aligned}(vw)^R(xu) &= (v^R \circ w^R)(xu) = (R_v \circ R_w)(xu) \\ &= R_v(xu \cdot w) = R_v(-xw \cdot w^{\perp}u) \\ &= -(xw \cdot w^{\perp}u) \cdot v = (xw \cdot v) \cdot v^{\perp}(w^{\perp}u) \\ &= (R_v \circ R_w)x \cdot (v^{\perp} \circ w^{\perp})u \\ &= (vw)^R x \cdot (vw)^T u\end{aligned}$$

(recall that $(vw)^T = v^{\perp} \circ w^{\perp}$). $\square$

The analogue of Proposition 3 also holds:

Proposition 5. *If orthogonal operators* A: $\mathbb{C}\mathrm{a}^{\oplus} \to \mathbb{C}\mathrm{a}^{\oplus}$ *and* B: $\mathbb{C}\mathrm{a}^2 \to \mathbb{C}\mathrm{a}^2$ *have the property that*

$$(11) \qquad B(xu) = Bx \cdot Au$$

for any elements $x \in \mathbb{C}\mathrm{a}^2$ and $u \in \mathbb{C}\mathrm{a}^{\oplus}$, *then they are necessarily unimodular and there is one and only one element* $a \in \operatorname{Spin}(9)$ *for which*

$$A = a^T,\ B = a^R. \tag{12}$$

As a preliminary we prove the following lemma:

Lemma 4. *If* B *is an orthogonal operator* $\mathbb{C}\mathrm{a}^2 \to \mathbb{C}\mathrm{a}^2$ *such that*

$$B(xu) = Bx \cdot u \tag{13}$$

for any elements $x \in \mathbb{C}\mathrm{a}^2$ *and* $u \in \mathbb{C}\mathrm{a}$ (*i.e. for* $u = \{0, \rho\}$, *where* $\rho \in \mathbb{C}\mathrm{a}$), *then* $B = \pm E$.

Proof. Let

$$Bx = \begin{cases} \{C\xi,\ C_1\xi\} & \text{if } x = \{\xi,\ 0\}, \\ \{D_1\eta,\ D\eta\} & \text{if } x = \{0,\ \eta\}, \end{cases}$$

and hence

$$Bx = \{C\xi + D_1\eta,\ C_1\xi + D\eta\} \quad \text{if} \quad x \in \{\xi,\ \eta\}.$$

In this notation relation (13), with $u = \{0, \rho\}$, becomes

$$\begin{aligned} \{C(\bar\rho,\ \bar\eta) + D_1(\bar\xi\bar\rho),\ C_1(\bar\rho,\ \bar\eta) + D(\bar\xi,\ \bar\rho) \\ = \{\bar\rho\,\overline{(C_1\xi + D\eta)},\ \overline{(C\xi + D_1\eta)}\,\bar\rho\}, \end{aligned}$$

from which it follows (first assuming $\xi = 0$ and then $\eta = 0$), that

$$\begin{gathered} C(\bar\rho\bar\eta) = \bar\rho \cdot \overline{D\eta},\ C_1(\bar\rho\bar\eta) = \overline{D_1\eta} \cdot \bar\rho, \\ D_1(\bar\xi\bar\rho) = \bar\rho \cdot \overline{C_1\xi},\ D(\bar\xi\bar\rho) = \overline{C\xi} \cdot \bar\rho. \end{gathered}$$

When $\rho = 1$ this yields

$$D_1\bar\xi = \overline{C_1\xi},\ D\bar\xi = \overline{C\xi}$$

and hence (replacing $\bar\rho$ by ρ and $\bar\eta$ by ξ)

$$C(\rho\xi) = \rho \cdot C\xi, \qquad C_1(\rho\xi) = C_1\xi \cdot \rho. \tag{14}$$

Therefore $C\rho = \rho c$ and $C_1\rho = c_1\rho$, where $c = C1$, $c_1 = C_1 1$, and hence identity (14) assumes the form

$$\rho\xi \cdot c = \rho \cdot \xi c, \qquad c_1 \cdot \rho\xi = c_1\rho \cdot \xi.$$

As we already know, the first identity yields $c \in \mathbb{R}$. But assuming in the second identity $c_1 = u + ve$, $\rho = w$ and $\xi = e$, where $u, v, w \in \mathbb{H}$, and considering that $(u + ve) \times we = -\bar{w}v + wu \cdot e$ and $(u + ve)\, e \cdot w = -\bar{w}u - wv \cdot e$, we obtain in the algebra $\mathbb{H}$ relations $\bar{w}v = \bar{w}u$, $wu = -wv$ possible for any w only when $u = v = 0$, i.e. for $c_1 = 0$. This proves that $C_1 = 0$ (and hence $D_1 = 0$) and that the operator C coincides with D and is an operator of multiplying by a real number c. Hence the operator B is also an operator of multiplying by c, which by virtue of the orthogonality of B is possible only if $c = \pm 1$. □

Proof of Proposition 5. If the operator A is unimodular and so there is an element $a \in \mathrm{Spin}\,(9)$ such that $A = a^T$, then relation (13) holds for the operator $B \circ (a^R)^{-1}$ (even for any u) and hence by Lemma 4 $B = \pm a^R = (\pm a)^R$. Since $(-a)^T = a^T$, this proves equations (11). The uniqueness of a in (11) follows from the fact that $b^T = a^T$ is possible only if $b = \pm a$ and $(-a)^R = -a^R \neq a^R$.

To complete the proof of Proposition 5 it thus remains to be established that identity (11) may hold only for a unimodular operator A. But if this identity holds for some nonunimodular orthogonal operator A, then it obviously does so for any other such operator (with a different B of course). It suffices therefore to arrive at a contradiction with the supposition that identity (11) holds for the operator A: $u \mapsto \bar{u}$, where $\bar{u} = \{-r, \rho\}$, if $u = \{r, \rho\}$, i.e. the supposition that there is an orthogonal operator B: $\mathbb{Ca}^2 \to \mathbb{Ca}^2$ such that

$$B\,(xu) = Bx \cdot \bar{u}. \tag{15}$$

When $u = \{0, \rho\}$ identity (15) coincides with (13) and so by Lemma 4, $B = \pm E$. Hence (15) is equivalent to the identity $xu = x\bar{u}$ which yields an absurd equation $u = \bar{u}$. This completes the proof of Proposition 5. □

Besides the octaves themselves one can consider, for example, matrices whose elements are octaves. Since there is a conjugation in the algebra $\mathbb{Ca}$, for any octave matrix X a *Hermitian conjugate matrix* X^* is defined that results from the transposed matrix $X^{(T)}$ if all its elements are replaced

by conjugate octaves. By analogy with the complex case the octave matrix X for which $X^* = X$ is called *Hermitian*.

On defining the product XY of octave matrices X and Y by the usual formula we at once see (after a calculation repeating completely the corresponding calculation for complex matrices) that for any octave matrices X and Y, just as for complex matrices, there is an equation $(XY)^* = Y^*X^*$, from which it follows immediately that the collection of all Hermitian octave matrices of a given order n is an algebra under the *Jordan multiplication*

$$X \circ Y = \frac{XY+YX}{2}.$$

That algebra is a commutative and unital one. Its identity element is the unit matrix E.

We study the algebra for $n = 3$. It derives its name $\mathbb{A}\mathrm{l}$ from the American mathematician Albert who was one of the first to pay attention to it.

Remark 6. The operation of Jordan multiplication has meaning in any algebra. It is obviously commutative and in an associative algebra it satisfies the identity

$$(x^2 \circ y) \circ x = x^2 \circ (y \circ x), \tag{16}$$

where $x^2 = x \circ x = xx$. Algebras with commutative multiplication that satisfy this identity are called *Jordan algebras*. (Incidentally, identity (16) holds in any alternative algebra, as was shown above in the proof of Lemma 1; therefore the commutative alternative algebra is Jordan.) Of course, since the octave algebra is nonassociative, there are no general reasons for the algebra of octave Hermitian matrices of order n to be a Jordan algebra. Nevertheless it turns out that because of the alternativity of the algebra $\mathbb{C}\mathrm{a}$ this algebra is nonetheless Jordan for $n \leqslant 3$, it being impossible, as was shown by Albert, to obtain it from any associative algebra for $n = 3$. This accounts for the particular role of $\mathbb{A}\mathrm{l}$ and for our interest in it. We shall not need, however, the Jordan property of $\mathbb{A}\mathrm{l}$ and shall not prove it.

Any element X of $\mathbb{A}\mathrm{l}$ can be represented uniquely as

$$X = a_1E_1 + a_2E_2 + a_3E_3 + X_1(\xi_1) + X_2(\xi_2) + X_3(\xi_3), \tag{17}$$

where

$$E_1=\begin{pmatrix}1&0&0\\0&0&0\\0&0&0\end{pmatrix},\ E_2=\begin{pmatrix}0&0&0\\0&1&0\\0&0&0\end{pmatrix},\ E_3=\begin{pmatrix}0&0&0\\0&0&0\\0&0&1\end{pmatrix}$$

and

$$X_1(\xi)=\begin{pmatrix}0&0&0\\0&0&\xi\\0&\bar\xi&0\end{pmatrix},\qquad X_2(\xi)=\begin{pmatrix}0&0&\bar\xi\\0&0&0\\\xi&0&0\end{pmatrix},$$

$$X_3(\xi)=\begin{pmatrix}0&\xi&0\\\bar\xi&0&0\\0&0&0\end{pmatrix},$$

and, as is shown by calculation,

$$E_i\circ E_j=\begin{cases}E_j & \text{if } j=i,\\ 0 & \text{if } j\neq i,\end{cases}\tag{18}$$

$$E_i\circ X_j(\xi)=\begin{cases}0 & \text{if } j=i,\\ \frac{1}{2}X_j(\xi) & \text{if } j\neq i,\end{cases}\tag{19}$$

$$X_i(\xi)\circ X_j(\eta)=\begin{cases}(\xi,\ \eta)(E-E_i) & \text{if } j=i,\\ X_{i+2}(\overline{\xi\eta}) & \text{if } j=i+1\end{cases}\tag{20}$$

(it is implied in the last formula that the indices are reduced mod 3; since by this convention $i = j + 1$ with $j = i + 2$, the case $j = i + 2$ reduces to the case $j = i + 1$).

This completely defines the algebraic structure of $\mathbb{A}1$.

One of the most important characteristics of an algebra is the structure of the set of its *idempotents*, i.e. of elements x for which $x^2 = x$. For the algebra $\mathbb{A}1$ we shall study the set of all its idempotents X whose trace $\operatorname{Tr} X$ is 1. Such idempotents will be called *primitive idempotents*.

For element (17) the condition $\operatorname{Tr} X = 1$ implies that

$$a_1 + a_2 + a_3 = 1\tag{21}$$

and the condition $X^2 = X$ is reduced to six equations

$$a_i^2 + |\xi_{i+1}|^2 + |\xi_{i+2}|^2 = a_i,$$
$$i = 1, 2, 3 \bmod 3,$$
$$\bar{\xi}_{i+2}\bar{\xi}_{i+1} + (a_{i+1} + a_{i+2})\,\xi_i = \xi_i,$$

equivalent by virtue of equation (21) to the equations

$$a_i\,(a_{i+1} + a_{i+2}) = |\xi_{i+1}|^2 + |\xi_{i+2}|^2, \quad i = 1, 2, 3 \bmod 3. \tag{22}$$

$$a_i\xi_i = \bar{\xi}_{i+1}\xi_{i+2}, \tag{23}$$

It follows from equations (23) that $a_i\,|\xi_i|^2 = \xi_i\xi_{i+1}\xi_{i+2}$ and at the same time that $a_i\,|\xi_i|^2 = \xi_{i+1}\xi_{i+2}\xi_i$. Hence the real number $\lambda = \xi_i\xi_{i+1}\xi_{i+2}$ remains unchanged when i is replaced by $i+1$ and hence is the same for all i, with

$$a_i\,|\xi_i|^2 = \lambda \quad \text{for every} \quad i = 1, 2, 3. \tag{24}$$

Now it can be easily seen that

$$|\xi_i|^2 = a_{i+1}a_{i+2} \quad \text{for any} \quad i = 1, 2, 3 \bmod 3. \tag{25}$$

Indeed, multiplying equation (22) by $a_{i+1}a_{i+2}$ yields by virtue of (24) the equation

$$a_ia_{i+1}a_{i+2}\,(a_{i+1} + a_{i+2}) = a_{i+2}\lambda + a_{i+1}\lambda,$$

from which it follows that $\lambda = a_ia_{i+1}a_{i+2}$ if $a_{i+1} + a_{i+2} \neq 0$, i.e. $a_i \neq 1$. Hence if in addition $a_i \neq 0$, then (25) follows from (24). If, however, $a_i = 0$ or $a_{i+1} + a_{i+2} = 0$, then it follows immediately from (22) that $\xi_{i+1} = \xi_{i+2} = 0$, and hence (25) follows from relation (22) for all $i + 1$. □

Conversely, if conditions (25) hold for all i, then for all i conditions (22) do. This proves that a *matrix $X \in$ Al is a primitive idempotent if and only if its elements satisfy conditions* (21), (23) *and* (25).

Notice that it follows immediately from (25) and (21) that for any $i = 1, 2, 3$ we have the inequality $a_i > 0$.

It can be shown without much difficulty that with $\xi_1, \xi_2, \xi_3 \in \mathbb{C}$ equations (21), (23) and (25) define a manifold diffeomorphic to a complex projective plane $\mathbb{C}P^2$ (the diffeomorphism $[z_1 : z_2 : z_3] \mapsto (\xi_1, \xi_2, \xi_3, a_1, a_2, a_3)$ is defined by

the formulas

$$\xi_i = \frac{z_{i+1}\bar{z}_{i+2}}{|z_1|^2 + |z_2|^3 + |z_3|^2}, \qquad a_i = \frac{|z_i|^2}{|z_1|^2 + |z_2|^2 + |z_3|^2},$$

where $i = 1, 2, 3 \bmod 3$) and with $\xi_1, \xi_2, \xi_3 \in \mathbb{H}$ they define a manifold diffeomorphic to a quaternion projective plane $\mathbb{H}\mathrm{P}^2$ (a projective n-dimensional space $\mathcal{A}\mathrm{P}^n$ over an algebra $\mathcal{A}$ is defined for any associative division algebra $\mathcal{A}$, and in particular for an algebra of quaternions $\mathbb{H}$, as a factor set of the set $\mathcal{A}^{n+1} \setminus \{0\}$ modulo the proportionality relation of vectors; the associativity is necessary for the transitivity of this relation). That is why the set of all primitive idempotents of an algebra $\mathbb{A}$l is called an *octave projective plane* and symbolized $\mathbb{C}\mathrm{aP}^2$. (There are also deeper reasons for this terminology; thus, see [11], one can define in $\mathbb{C}\mathrm{a}\ \mathrm{P}^2$ "straight lines" that are in fact 8-dimensional spheres for which the incidence axioms of projective geometry are true; but all this is beyond the scope of our presentation.)

Let U_i, $i = 1, 2, 3$, be an open subset of $\mathbb{C}\mathrm{a}\ \mathrm{P}^2$ consisting of points $(\xi_1, \xi_2, \xi_3, a_1, a_2, a_3)$ for which $a_3 \neq 0$. It is easily seen that that set is diffeomorphic to the product $\mathbb{C}\mathrm{a} \times \mathbb{C}\mathrm{a} \approx \mathbb{R}^{16}$ (for $i = 3$, for example, the diffeomorphism $\mathbb{C}\mathrm{a} \times \mathbb{C}\mathrm{a} \to U_3$ is given by the formulas

$$\xi_1 = \frac{\eta_2}{1 + |\eta_1|^2 + |\eta_2|^2}, \qquad \xi_2 = \frac{\eta_1}{1 + |\eta_1|^2 + |\eta_2|^2},$$

$$\xi_3 = \frac{\bar{\eta}_1\bar{\eta}_2}{1 + |\eta_1|^2 + |\eta_2|^2}, \qquad a_1 = \frac{|\eta_1|^2}{1 + |\eta_1|^2 + |\eta_2|^2},$$

$$a_2 = \frac{|\eta_2|^2}{1 + |\eta_1|^2 + |\eta_2|^2}, \qquad a_3 = \frac{1}{1 + |\eta_1|^2 + |\eta_2|^2},$$

where $\eta_1, \eta_2 \in \mathbb{C}\mathrm{a}$) and is hence simply connected. Since the intersections $U_1 \cap U_2$ and $(U_1 \cap U_2) \cap U_3$ are obviously connected (the former is diffeomorphic to the product $\mathbb{C}\mathrm{a} \times (\mathbb{C}\mathrm{a} \setminus \{0\})$ and the latter to $(\mathbb{C}\mathrm{a} \setminus \{0\}) \times (\mathbb{C}\mathrm{a} \setminus \{0\})$), $\mathbb{C}\mathrm{a}\ \mathrm{P}^2 = U_1 \cup U_2 \cup U_3$, from which it follows that the *octave projective plane* $\mathbb{C}\mathrm{a}\ \mathrm{P}^2$ *is a connected and simply connected manifold* (of dimension 16).

Lecture 16

Scalar products in the algebra $\mathbb{A}\mathrm{l}$ *· Automorphisms and differentiations of the algebra* $\mathbb{A}\mathrm{l}$ *· Adjoint differentiations of the algebra* $\mathbb{A}\mathrm{l}$ *· The Freudenthal theorem · Consequences of the Freudenthal theorem · The Lie group* F_4 *· The Lie algebra* $\mathfrak{f}_4$ *· The structure of the Lie algebra* $\mathfrak{f}_4^{\mathbb{C}}$

The statement that for an element X of the algebra $\mathbb{A}\mathrm{l}$, there is an equation

$$X = a_1E_1 + a_2E_2 + a_3E_3 + X_1(\xi_1) + X_2(\xi_2) + X_3(\xi_3)$$

(see formula (17) of Lecture 15) implies that the vector space $\mathbb{A}\mathrm{l}$ is a direct sum of three vector spaces $\mathbb{R}$ and three vector spaces $\mathbb{C}\mathrm{a}$ (so that in particular $\dim \mathbb{A}\mathrm{l} = 3 + 3\cdot 8 = 27$). Since vector spaces $\mathbb{R}$ and $\mathbb{C}\mathrm{a}$ are Euclidean, it follows that a Euclidean structure (a scalar product) is defined in the vector space $\mathbb{A}\mathrm{l}$ as well. For the norm (the length) $|X|$ of an element X of $\mathbb{A}\mathrm{l}$ we have the formula

$$(1) \quad |X|^2 = a_1^2 + a_2^2 + a_3^2 + |\xi_1|^2 + |\xi_2|^2 + |\xi_3|^2.$$

The scalar product (X, Y) of elements X, Y of $\mathbb{A}\mathrm{l}$ can be expressed in terms of their Jordan product by the formula

$$(2) \qquad (X, Y) = \mathrm{Tr}\,(X \circ Y)$$

which can be immediately verified by a direct calculation.

From this formula it follows in particular that *the idempotent* $X \in \mathbb{A}\mathrm{l}$ *is primitive if and only if* $|X| = 1$.

Note that we introduce no conjugation into $\mathbb{A}\mathrm{l}$, so that $\mathbb{A}\mathrm{l}$ is not a metric algebra. Nor can it be a normed algebra by virtue of the Hurwitz theorem.

Besides the scalar product, the algebra $\mathcal{A}l$ carries another important functional, to construct it we must start somewhat from afar.

Since in view of skew-commutativity the associator $(ax)\,y - a\,(xy)$ changes sign under the interchanging $(a, x, y) \mapsto (y, a, x)$, in any alternative algebra there is an identity

$$(ax)\,y + y\,(ax) = a\,(xy) + (ya)\,x.$$

Denoting the element a by a_i^j, the element x by x_j^k and the element y by y_k^i we can write the identity as

$$(a_i^j x_j^k)\,y_k^i + y_k^i\,(a_i^j x_j^k) = a_i^j\,(x_j^k y_k^i) + (y_k^i a_i^j)\,x_j^k.$$

It obviously remains valid if the summation is extended with respect to all indices from 1 to n (we need only the case $n = 3$, though). But introducing matrices $A = (a_i^j)$, $X = (x_j^k)$ and $Y = (y_k^i)$ we can write the resulting identity as

$$(3)\ \mathrm{Tr}\,(AX \circ Y) + \mathrm{Tr}\,(Y \circ AX) = \mathrm{Tr}\,(A \circ XY) + \mathrm{Tr}\,(YA \circ X)$$

which is true for any matrices with elements in an arbitrary alternative algebra and hence, in particular, for matrices in $\mathcal{A}l$.

Notice that this method has a quite general character and is applicable to any multilinear identity. Denoting, for example, by $\mathrm{Re}\,\xi$ the coefficient of 1 in an octave ξ, i.e. the scalar product $(\xi, 1)$, we obtain an identity

$$\mathrm{Re}\,(ab) = \mathrm{Re}\,(ba)$$

which is true for any octaves a and b. For matrices over octaves therefore there is an identity

$$(4) \qquad \mathrm{Re}\,\mathrm{Tr}\,(AB) = \mathrm{Re}\,\mathrm{Tr}\,(BA)$$

which implies that after applying Re Tr the multiplication of octave matrices becomes commutative.

By commutativity, identity (3) yields the identity

$$2\,\mathrm{Re}\,\mathrm{Tr}\,(AX \cdot Y) = \mathrm{Re}\,\mathrm{Tr}\,(A \cdot XY) + \mathrm{Re}\,\mathrm{Tr}\,(YA \cdot X).$$

By a cyclic permutation here of A, X and Y, we next obtain an identity

$$2\,\mathrm{Re}\,\mathrm{Tr}\,(XY \cdot A) = \mathrm{Re}\,\mathrm{Tr}\,(X \cdot YA) + \mathrm{Re}\,\mathrm{Tr}\,(AX \cdot Y).$$

Subtracting these identities from each other and using again commutativity we obtain, after dividing by 3, an identity

(5) $$\operatorname{Re}\operatorname{Tr}(AX\cdot Y)=\operatorname{Re}\operatorname{Tr}(A\cdot XY)$$

which implies that, after dividing by Re Tr, the multiplication of octave matrices becomes also associative.

So does the Jordan multiplication of octave matrices:

$$\begin{aligned}\operatorname{Re}\operatorname{Tr}((A\circ X)\circ Y)&=\operatorname{Re}\operatorname{Tr}((A\circ X)\circ Y)\\&=\frac{1}{2}[\operatorname{Re}\operatorname{Tr}(AX\cdot Y)+\operatorname{Re}\operatorname{Tr}(Y\cdot XA)]\\&=\frac{1}{2}[\operatorname{Re}\operatorname{Tr}(A\cdot XY)+\operatorname{Re}\operatorname{Tr}(YX\cdot A)]\\&=\operatorname{Re}\operatorname{Tr}(A\cdot(X\circ Y))=\operatorname{Re}\operatorname{Tr}(A\circ(X\circ Y)).\end{aligned}$$

Since for matrices in $\mathbb{A}l$ the trace is real it finally follows that

$$\operatorname{Tr}((A\circ X)\circ Y)=\operatorname{Tr}(A\circ(X\circ Y))$$

for any matrices A, X, $Y\in\mathbb{A}l$. In view of formula (2) this means that in $\mathbb{A}l$ there is an identity

$$(A\circ X,\ Y)=(A,\ X\circ Y)$$

from which it follows (by the commutativity of $\mathbb{A}l$) that the *trilinear functional*

(6) $$(X,Y,Z)=\operatorname{Tr}((X\circ Y)\circ Z)=(X\circ Y,Z),\quad X,\ Y,\ Z\in\mathbb{A}l,$$

is symmetric in X, Y and Z.

We shall call functional (6) a *scalar triproduct.*

If an automorphism $\Phi\colon\mathbb{A}l\to\mathbb{A}l$ of the algebra $\mathbb{A}l$ *preserves the trace*, i.e. if $\operatorname{Tr}(\Phi X)=\operatorname{Tr}X$ for any element $X\in\mathbb{A}l$, then, of course, it does both scalar products,

(7) $$(\Phi X,\Phi Y)=(X,Y)\ \text{ and }\ (\Phi X,\Phi Y,\Phi Z)=(X,Y,Z),$$

for any of elements X, Y, $Z\in\mathbb{A}l$.

It follows in particular that the group of all trace-preserving automorphisms of the algebra is a closed subgroup of the orthogonal group O (27) and so is a compact Lie group. We shall denote this group, for reasons to be explained in

Semester VI, by F_4 and its Lie algebra by $\mathfrak{f}_4$. Elements of the Lie algebra $\mathfrak{f}_4$ are differentiations D: $\mathbb{A}\mathrm{l} \to \mathbb{A}\mathrm{l}$ *annulling the trace*, i.e. such that $\operatorname{Tr}(DA) = 0$ for any matrix $A \in \mathbb{A}\mathrm{l}$.

Remark 1. We show below that any automorphism preserves the trace, so that in fact the group F_4 is the group of *all* automorphisms of the algebra $\mathbb{A}\mathrm{l}$ but it is convenient for us to postpone the proof of this fact for the time being.

It is remarkable that, conversely, any linear operator Φ: $\mathbb{A}\mathrm{l} \to \mathbb{A}\mathrm{l}$ *preserving both scalar products is a trace-preserving automorphism of the algebra* $\mathbb{A}\mathrm{l}$. Indeed

$$(\Phi X \circ \Phi Y - \Phi(X \circ Y), \Phi Z) = (\Phi X, \Phi Y, \Phi Z) - (\Phi(X \circ Y), \Phi Z) = (X, Y, Z) - (X \circ Y, Z) = 0$$

for any $X, Y, Z \in \mathbb{A}\mathrm{l}$ and hence $\Phi X \circ \Phi Y = \Phi(X \circ Y)$, because the operator Φ is singular, being an isometry with respect to the scalar product (2) and therefore any element of $\mathbb{A}\mathrm{l}$ can be represented as ΦZ. This proves that the operator Φ is an automorphism of $\mathbb{A}\mathrm{l}$. Therefore $\Phi E = E$ and hence $\operatorname{Tr}(\Phi X) = \operatorname{Tr} X$, since $\operatorname{Tr} X = (X, E)$ for any $X \in \mathbb{A}\mathrm{l}$. $\square$

Thus irrespective of the algebra $\mathbb{A}\mathrm{l}$ the group F_4 can be characterized as a group of isometries of a 27-dimensional Euclidean space that preserve some trilinear functional.

As we know, preserving a scalar product (isometry) for operators Φ of the form e^{tD} is equivalent to the skew-symmetry of the operator D, i.e. to the identity

$$(DX, Y) + (X, DY) = 0.$$

Similarly, preserving the scalar triproduct is equivalent to the identity

$$(DX, Y, Z) + (X, DY, Z) + (X, Y, DZ) = 0 \tag{8}$$

for any elements $X, Y, Z \in \mathbb{A}\mathrm{l}$. Indeed, differentiating the function $f(t) = (e^{tD}X, e^{tD}Y, e^{tD}Z)$ with respect to t, we immediately find by virtue of linearity that $f'(0)$ is equal to the left-hand side of identity (8). Therefore if $f(t) =$ const, then (7) holds. Conversely, if (8) holds, then $f'(t) = 0$ for all t and therefore $f(t) =$ const, which is equivalent to the second identity of (7). $\square$

By analogy, linear operators D satisfying identity (8) will be called *skew-symmetric with respect to the scalar triple product* (6).

According to the foregoing a *linear operator* D: $\mathbb{A}l \to \mathbb{A}l$ *is a trace-nullifying differentiation of the algebra* $\mathbb{A}l$ (*i.e. it is in the Lie algebra* $\mathfrak{f}_4$) *if and only if it is skew-symmetric with respect to both scalar products* (2) *and* (6).

An octave matrix A is said to be *skew Hermitian* if $A^* = -A$. A direct calculation shows that if A is a skew Hermitian matrix, then for any Hermitian matrix X the matrix $[A, X] = AX - XA$ is also Hermitian. Thus any skew Hermitian matrix A of order 3 defines some linear operator ad A: $\mathbb{A}l \to \mathbb{A}l$ by the formula

$$(\mathrm{ad}\, A)\, X = [A, X], \qquad X \in \mathbb{A}l.$$

Since by identities (3) and (5), for any octave matrices, $\mathrm{Re\,Tr}\,([A, X] \circ Y) = \mathrm{Re\,Tr}\,([A, X]\, Y)$

$$\begin{aligned}
&= \mathrm{Re\,Tr}\,(AX \cdot Y) - \mathrm{Re\,Tr}\,(XA \cdot Y)\\
&= \mathrm{Re\,Tr}\,(Y \cdot AX) - \mathrm{Re\,Tr}\,(X \cdot AY)\\
&= \mathrm{Re\,Tr}\,(YA \cdot X) - \mathrm{Re\,Tr}\,(X \cdot AY)\\
&= -\mathrm{Re\,Tr}\,(X \cdot [A, Y]) = -\mathrm{Re\,Tr}\,(X \circ [A, Y]),
\end{aligned}$$

we have, given $X, Y \in \mathbb{A}l$ for any skew Hermitian matrix A

$$([A, X], Y) + (X, [A, Y]) = 0,$$

an equation implying that ad A is skew-symmetric with respect to the scalar product (2).

Further, as we know, in an alternative algebra the associative relation holds for elements a, b, c, if there are identical elements among them. It also holds, of course, if at least one element a, b, c is in $\mathbb{R}$ from which it follows its validity if there are conjugate elements among a, b, c. Applying this fact to the elements of a matrix $X(XX) - (XX)X$, where $X = (x_i^j)$ is an octave Hermitian $n \times n$ matrix, enables us to assume that in the expressions $x_i^j (x_j^k x_k^l) - (x_i^j x_j^k)\, x_k^l$ of nonzero elements the summation over j and k is extended only to different indices j and k other than i and l. For $n = 3$ therefore i is necessarily equal to l, so that for any matrix $X \in \mathbb{A}l$ the matrix $X(XX) -$

$(XX)\,X$ is necessarily diagonal, i.e. is of the form

$$\begin{pmatrix} \alpha & 0 & 0 \\ 0 & \beta & 0 \\ 0 & 0 & \gamma \end{pmatrix}, \text{ where } \alpha,\ \beta,\ \gamma \in \mathbb{C}a.$$

If a matrix X is of the form (1), then for octaves α, β, γ, there are formulas

$$\alpha = \xi_3(\xi_1\xi_2) + \bar{\xi}_2(\bar{\xi}_2\bar{\xi}_3) - (\xi_3\xi_1)\,\xi_2 - (\bar{\xi}_2\bar{\xi}_1)\,\bar{\xi}_3,$$
$$\beta = \xi_1(\xi_2\xi_3) + \bar{\xi}_3(\bar{\xi}_2\bar{\xi}_1) - (\xi_1\xi_2)\,\xi_3 - (\bar{\xi}_3\bar{\xi}_2)\bar{\xi}_1,$$
$$\gamma = \xi_2(\xi_3\xi_1) + \bar{\xi}_1(\bar{\xi}_3\bar{\xi}_2) - (\xi_2\xi_3)\,\xi_1 - (\bar{\xi}_1\bar{\xi}_3)\,\bar{\xi}_2$$

from which by virtue of the skew-symmetric of the associators it follows that $\alpha = \beta = \gamma$.

Since for any octave matrix A there is an equation $\operatorname{Tr}(A\cdot\alpha E) = \operatorname{Tr} A\cdot\alpha$ and hence $\operatorname{Tr}(A\cdot\alpha E) = 0$ when $\operatorname{Tr} A = 0$, it follows that for any skew-Hermitian matrix A of order 3 with a trace equal to zero and for any matrix $X \in \mathbb{A}\mathrm{l}$ we have

$$\operatorname{Tr}(A\cdot X\,(XX)) = \operatorname{Tr}(A\cdot(XX)\,X)$$

and therefore (see formulas (4) and (5)) also an equation

$$\operatorname{Re}\operatorname{Tr}(AX\cdot XX) = \operatorname{Re}\operatorname{Tr}(XA\cdot XX)$$

which implies that

$$\operatorname{Re}\operatorname{Tr}((\operatorname{ad} A)\,X\cdot XX) = 0,$$

i.e. (since $(\operatorname{ad} A)\,X \in \mathbb{A}\mathrm{l}$ and $XX = X \circ X$) that

$$((\operatorname{ad} A)\,X,\ X,\ X) = 0.$$

Polarizing the obtained identity by X we find at once that for the linear mapping $\operatorname{ad} A\colon \mathbb{A}\mathrm{l} \to \mathbb{A}\mathrm{l}$ we have identity (8).

Thus $\operatorname{ad} A$ is skew-symmetric with respect to both scalar products (2) and (6). Hence it is a trace-nullifying differentiation of the algebra $\mathbb{A}\mathrm{l}$.

The vector space of all skew-symmetric octave matrices of order 3 with a trace equal to zero will be symbolized $\mathbb{M}$. According to the foregoing, *for any matrix* $A \in \mathbb{M}$ *the linear operator* $\operatorname{ad} A$ *is in the Lie algebra* $\mathfrak{f}_4$. The resulting (obvious-

ly linear) mapping

$$\mathrm{ad}\colon\ \mathbb{M} \to \mathfrak{f}_4$$

is injective. Indeed, a trivial calculation shows that only scalar matrices of the form aE, with $a \in \mathbb{R}$ are commutative with every matrix in $\mathbb{A}1$ and such a matrix has a zero trace only for $a = 0$. $\square$

Differentiations of $\mathbb{A}1$ of the form $\mathrm{ad}\, A$, $A \in \mathbb{M}$, will be called *adjoint differentiations.*

Of particular importance to us will be matrices in $\mathbb{M}$ all of whose diagonal elements are zero. These matrices constitute a vector subspace $\mathbb{M}^0$ of the space $\mathbb{M}$. Let

$$Y_1(\eta) = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & \eta \\ 0 & -\bar{\eta} & 0 \end{pmatrix}, \quad Y_2(\eta) = \begin{pmatrix} 0 & 0 & -\bar{\eta} \\ 0 & 0 & 0 \\ \eta & 0 & 0 \end{pmatrix},$$

$$Y_3(\eta) = \begin{pmatrix} 0 & \eta & 0 \\ -\bar{\eta} & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Then any matrix $A \in \mathbb{M}^0$ can be uniquely written as

$$A = Y_1(\eta_1) + Y_2(\eta_2) + Y_3(\eta_3), \quad \eta_1, \eta_2, \eta_3 \in \mathbb{C}\mathrm{a},$$

from which it follows in particular that $\dim \mathbb{M}^0 = 24$.

Now we can prove the important Freudenthal theorem which makes the study of $\mathbb{A}1$ and F_4 significantly easier. As ever $(F_4)_e$ denotes the component of the identity of F_4.

Proposition 1 (Freudenthal theorem). *For any element $X \in \mathbb{A}1$ there is an automorphism $\Phi \in (F_4)_e$ such that*

$$\Phi X = \lambda_1 E_1 + \lambda_2 E_2 + \lambda_3 E_3, \quad \textit{where} \quad \lambda_1 \leqslant \lambda_2 \leqslant \lambda_3.$$

The numbers $\lambda_1 \leqslant \lambda_2 \leqslant \lambda_3$ are uniquely defined by X.

Two elements of $\mathbb{A}1$ can be sent to each other by an automorphism in $(F_4)_e$ if and only if the corresponding numbers $\lambda_1 \leqslant \lambda_2 \leqslant \lambda_3$ coincide.

In terms of the theory of transformation groups this statement says that *every orbit of the group $(F_4)_e$ in $\mathbb{A}1$ contains a unique diagonal matrix $\lambda_1 E_1 + \lambda_2 E_2 + \lambda_3 E_3$ for which $\lambda_1 \leqslant \lambda_2 \leqslant \lambda_3$.* It is in this form that we shall prove the statement.

Being a closed subgroup of a compact group SO(26) the group $(F_4)_e$ is compact. Therefore in any orbit of it there is a matrix X of the form (1) for which the sum $a_1^2 + a_2^2 + a_3^2$ has the largest value (on that orbit). It turns out that *such a matrix is always a diagonal one.*

Indeed, for any matrix $A \in \mathrm{Al}$ and any $t \in \mathbb{R}$ the matrix $X_t = e^{t\,\mathrm{ad}\,A}X$ is in the orbit of X (since $\mathrm{ad}\,A \in \mathfrak{f}_4$ and hence $e^{t\,\mathrm{ad}\,A} \in (F_4)_e$) and therefore for its diagonal elements $a_1(t)$, $a_2(t)$, $a_3(t)$ we have $f(t) \leqslant f(0)$, where $f(t) = a_1(t)^2 + a_2(t)^2 + a_3(t)^2$. But, as we know (see p. 49), X_t is a solution of the matrix differential equation

$$\frac{dX_t}{dt} = (\mathrm{ad}\,A)\,X_t, \qquad X_0 = X,$$

equivalent to three differential equations for octave elements $\xi_1(t)$, $\xi_2(t)$ and $\xi_3(t)$ of X_t and to three differential equations for its number elements $a_1(t)$, $a_2(t)$, $a_3(t)$. In the case, where $A = Y_1(\eta)$ these equations are shown by a simple calculation using formula (2) of Lecture 14, to be of the form

$$(9)\qquad \begin{aligned} &\frac{da_1(t)}{dt} = 0, && \frac{d\xi_1(t)}{dt} = (a_3(t) - a_1(t))\,\eta, \\ &\frac{da_2(t)}{dt} = 2(\eta, \xi_1(t)), && \frac{d\xi_2(t)}{dt} = -\bar{\eta}\overline{\xi_3(t)}, \\ &\frac{da_3(t)}{dt} = -2(\eta, \xi_1(t)), && \frac{d\xi_3(t)}{dt} = \overline{\xi_2(t)}\,\bar{\eta}. \end{aligned}$$

Hence $a_1(t) = \mathrm{const}$ and $a_2(t) + a_3(t) = \mathrm{const}$. In addition $f'(t) = 2(a_1'(t)\,a_1(t) + a_2'(t)\,a_2(t) + a_3'(t)\,a_3(t)) = 4(\eta, \xi_1(t))\,(a_2(t) - a_3(t))$ from which it follows by equation $f'(0) = 0$ that for $(\eta, \xi_1(0)) \neq 0$ we have $a_2(0) = a_3(0)$. Therefore $a_1(t) = a_1(0)$ and $a_2(t) + a_3(t) = 2a_2(0)$ and hence $f(t) = f(0) + 2(a_3(0) - a_3(t))^2$, which is possible, in view of $f(t) \leqslant f(0)$, only when $a_3(t) = a_3(0)$. Then $a_3'(t) = 0$ and hence $(\eta, \xi_1(t)) = 0$, which contradicts the condition $(\eta, \xi_1(0)) \neq 0$ when $t = 0$. Consequently,

$$(\eta, \xi_1(0)) = 0$$

for any octave η which is possible only when $\xi_1(0) = 0$.

In a similar fashion it can be proved that $\xi_2(0) = 0$ and $\xi_3(0) = 0$. Hence the matrix $X = X_0$ is a diagonal one. □

We now show that *any diagonal matrix* $X = a_1E_1 + a_2E_2 + a_3E_3$ *can be transformed by an automorphism in* $(F_4)_e$ *again into a diagonal matrix for which* $a_1 \leqslant a_2 \leqslant a_3$. It is clear that to do this it suffices to prove that it is possible to interchange in the diagonal matrix $X = a_1E_1 + a_2E_2 + a_3E_3$ by using an automorphism in $(F_4)_e$ any two diagonal elements, say, a_2 and a_3. To this end we again consider the matrix $X_t = e^{t\,\mathrm{ad}\,A}X$ with $A = Y_1(\eta)$. It follows immediately from equations (9) that for this matrix the function $a_2(t) - a_3(t)$ satisfies the differential equation

$$\frac{d^2(a_2(t)-a_3(t))}{dt^2} = 4(\eta, \eta)(a_2(t)-a_3(t))$$

with the initial condition $a_2'(0) - a_3'(0) = 0$ (since $\xi_1(0) = 0$ by virtue of X being a diagonal matrix). Hence

$$a_2(t) - a_3(t) = (a_2(0) - a_3(0)) \cos 2\,|\,\eta\,|\,t.$$

Assuming for simplicity that $|\,\eta\,| = 1$ it follows in particular that

$$a_2\left(\frac{\pi}{2}\right) - a_3\left(\frac{\pi}{2}\right) = -(a_2(0) - a_3(0))$$

and hence (since $a_2(t) + a_3(t) = \mathrm{const}$) that $a_2\left(\frac{\pi}{2}\right) = a_3(0) = a_3$ and $a_3\left(\frac{\pi}{2}\right) = a_2(0) = a_2$. Thus the automorphism $e^{\frac{\pi}{2}\,\mathrm{ad}\,Y_1(\eta)}$ (for any η with $|\eta| = 1$) does interchange a_2 and a_3. $\square$

This completes the proof of the first statement of Proposition 1. By that statement to every matrix $X \in \mathbb{A}\mathrm{l}$ there correspond (possibly not uniquely) three numbers, $\lambda_1 \leqslant \lambda_2 \leqslant \lambda_3$, having the property that $\Phi X = \lambda_1E_1 + \lambda_2E_2 + \lambda_3E_3$ for some automorphism $\Phi \in (F_4)_e$.

Lemma 1. *There are equations*

$$\lambda_1 + \lambda_2 + \lambda_3 = (X, E),$$
$$\lambda_1^2 + \lambda_2^2 + \lambda_3^2 = (X, X),$$
$$\lambda_1^3 + \lambda_2^3 + \lambda_3^3 = (X, X, X).$$

Proof. For the diagonal matrix ΦX these equations are obvious (since $(X, E) = \mathrm{Tr}\,X$, $(X, X) = \mathrm{Tr}\,(X \circ X)$ and

$(X, X, X) = \mathrm{Tr}\,(X \circ X \circ X)$. Since $(\Phi X, E) = (\Phi X, \Phi E) = (X, E)$, $(\Phi X, \Phi X) = (X, X)$ and $(\Phi X, \Phi X, \Phi X) = (X, X, X)$, they are true also for any matrix $X \in \mathbb{A}\mathrm{l}$. □

Now we are in a position to complete the proof of Proposition 1.

Proof of Proposition 1. Since the first statement of Proposition 1 is already proved and the third is immediate from the first two, it remains to prove only the second statement. This follows immediately from Lemma 1, since by the well-known formulas of the theory of symmetric polynomials, the numbers λ_1, λ_2, λ_3 can be restored uniquely up to an order from the number $\sigma_k = \lambda_1^k + \lambda_2^k + \lambda_3^k$, $k = 1, 2, 3$. □

Numbers $\lambda_1 \leqslant \lambda_2 \leqslant \lambda_3$ will be called *eigenvalues of an octave matrix* X. We emphasize that their sum is equal to the trace $\mathrm{Tr}\, X$ of that matrix.

The Freudenthal theorem makes the study of the algebra $\mathbb{A}\mathrm{l}$ significantly easier. It follows immediately from it, for example, that the *degrees of any element* $X \in \mathbb{A}\mathrm{l}$ *are associative*, i.e. that for every $X \in \mathbb{A}\mathrm{l}$ all n-fold products of the element by itself are the same regardless of bracket arrangement, since this is obviously the case for a diagonal matrix X. (In a similar fashion we can also prove for $\mathbb{A}\mathrm{l}$ the Jordan identity (16) in Lecture 15, for in the case where one of the factors is diagonal (16) is obvious.)

The degrees being associative, the *nth degree* X^n of an element $X \in \mathbb{A}\mathrm{l}$ is correctly defined for every $n \geqslant 0$. Therefore for any polynomial $p\,(T)$ with real coefficients the same holds true for an element $p\,(X) \in \mathbb{A}\mathrm{l}$. If $p\,(x) = 0$, then the polynomial $p\,(T)$ is called the *nullifying polynomial of the element* X.

A nullifying polynomial of least degree with the leading coefficient equal to 1 is referred to as a *minimal polynomial* of an element $X \in \mathbb{A}\mathrm{l}$. It is obvious that it is uniquely defined and that for any authomorphism $\Phi\colon \mathbb{A}\mathrm{l} \to \mathbb{A}\mathrm{l}$ (which is not assumed to preserve the trace) the *minimal polynomials of the elements* X *and* ΦX *are the same.*

If X is a diagonal matrix, then its diagonal elements are roots of every nullifying polynomial and conversely any polynomial whose roots are these elements nullifies the matrix X. It follows that *for any matrix* $X \in \mathbb{A}\mathrm{l}$ *the degree*

of its minimal polynomial is at most three, the degree being three if and only if the eigenvalues of the matrix X are all different.

In addition we see that in the last case the coefficient of T^2 in the minimal polynomial is $-(\lambda_1 + \lambda_2 + \lambda_3) = -\mathrm{Tr}\, X$. Hence by the invariance of the minimal polynomial, for any automorphism Φ: $\mathbb{A}\mathrm{l} \to \mathbb{A}\mathrm{l}$ we have

$$\mathrm{Tr}\, \Phi X = \mathrm{Tr}\, X.$$

By continuity, that equation remains valid also when some eigenvalues of X coincide. This proves that *any automorphism of* $\mathbb{A}\mathrm{l}$ *is trace-preserving*, i.e. that F_4 is the group $\mathrm{Aut}\, \mathbb{A}\mathrm{l}$ of all automorphisms of $\mathbb{A}\mathrm{l}$.

It is also immediate from the Freudenthal theorem that F_4 *acts transitively in the octave projective plane* $\mathbb{C}\mathrm{aP}^2$ *of primitive idempotents of* $\mathbb{A}\mathrm{l}$, i.e. any primitive idempotent can be sent by some automorphism to any other primitive idempotent. It is clear that a diagonal matrix is an idempotent if and only if all its diagonal elements are 0 or 1. The eigenvalues of a primitive idempotent are therefore 0, 0, 1 and hence every such idempotent can be sent to an idempotent E_3 by some automorphism. □

This means that the *octave projective plane* $\mathbb{C}\mathrm{aP}^2$ *is homeomorphic to the quotient manifold* F_4/K *of the Lie group* F_4 *mod its subgroup* K which leaves fixed some primitive idempotent, say for definiteness, an idempotent E_1.

Let $\Phi \in K$. Since $\Phi E_1 = E_1$, Φ sends to itself the annulet $\mathrm{Ann}\, E_1$ of the element E_1, i.e. the vector space of all elements $X \in \mathbb{A}\mathrm{l}$ such that $X \circ E_1 = 0$. It is easy to see however that $\mathrm{Ann}\, E_1$ consists of elements (1) for which $a_1 = 0$ and $\xi_2 = \xi_3 = 0$ and so is a direct sum of a one-dimensional subspace of matrices of the form $a\,(E_2 + E_3)$ and the subspace $\mathrm{Ann}^0\, E_1$ which consists of matrices of the form

$$X = r\,(E_2 - E_3) + X_1\,(\rho), \quad \text{where} \quad r \in \mathbb{R}, \quad \rho \in \mathbb{C}\mathrm{a}.$$

Since the operator Φ is orthogonal and $\Phi\,(E_2 + E_3) = \Phi\,(E - E_1) = E - E_1 = E_2 + E_3$, it follows that the automorphism Φ sends to itself the subspace $\mathrm{Ann}^0\, E_1$ and therefore induces some orthogonal operator

$$\Phi^0 : \ \mathrm{Ann}^0\, E_1 \to \mathrm{Ann}^0\, E_1.$$

Similarly the automorphism Φ sends to itself the vector space $\mathscr{E}$ of all elements $X \in \mathbb{A}\mathrm{l}$ for which $2E_1 \circ X = X$ and so induces some orthogonal operator

$$\Phi' \colon \mathscr{E} \to \mathscr{E}.$$

As is immediate from formulas (18) to (20) of the preceding lecture, $\mathscr{E}$ consists of all matrices of the form $X_2(\xi) + X_3(\eta)$, $\xi, \eta \in \mathbb{C}\mathrm{a}$, and therefore the algebra $\mathbb{A}\mathrm{l}$ can be decomposed into a direct sum of two vector spaces $\mathscr{E}$ and $\mathrm{Ann}^0 E_1$ and two one-dimensional vector spaces generated by the elements E_1 and $E_2 + E_3$. Hence the *automorphism* Φ *is uniquely defined by the operators* Φ^0 *and* Φ'.

We also see that the vector space $\mathscr{E}$ is naturally isomorphic to the vector space $\mathbb{C}\mathrm{a}^2$ of octave pairs $\{\xi, \eta\}$ while the vector space $\mathrm{Ann}^0 E_1$ is isomorphic to the vector space $\mathbb{C}\mathrm{a}^{\oplus}$ of pairs $\{r, \rho\}$, where $r \in \mathbb{R}$ and $\rho \in \mathbb{C}\mathrm{a}$. The operators Φ' and Φ^0 therefore can be regarded as the operators $\mathbb{C}\mathrm{a}^2 \to \mathbb{C}\mathrm{a}^2$ and $\mathbb{C}\mathrm{a}^{\oplus} \to \mathbb{C}\mathrm{a}^{\oplus}$, respectively. Given any elements $x = \{\xi, \eta\}$ in $\mathbb{C}\mathrm{a}^2$ and $u = \{r, \rho\}$ in $\mathbb{C}\mathrm{a}^{\oplus}$ the element $xu = \{-r\xi + \overline{\rho}\overline{\eta}, r\eta + \overline{\xi}\overline{\rho}\}$ in $\mathbb{C}\mathrm{a}^2$ will have in $\mathscr{E}$ the corresponding matrix

$$\begin{pmatrix} 0 & r\eta + \overline{\xi}\overline{\rho} & -r\overline{\xi} + \eta\rho \\ r\overline{\eta} + \rho\xi & 0 & 0 \\ -r\xi + \overline{\rho}\overline{\eta} & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & \eta & \overline{\xi} \\ \overline{\eta} & 0 & 0 \\ \xi & 0 & 0 \end{pmatrix} \circ \begin{pmatrix} 0 & 0 & 0 \\ 0 & r & \rho \\ 0 & \overline{\rho} & -r \end{pmatrix},$$

which is a Jordan product of the matrices in $\mathscr{E}$ and $\mathrm{Ann}^0 E_1$ which correspond to elements x and u. Since Φ' and Φ^0 are induced by an automorphism Φ of $\mathbb{A}\mathrm{l}$, for these operators (regarded as operators $\mathbb{C}\mathrm{a}^2 \to \mathbb{C}\mathrm{a}^2$ and $\mathbb{C}\mathrm{a}^{\oplus} \to \mathbb{C}\mathrm{a}^{\oplus}$) there is an identity

$$(10) \qquad \Phi'(xu) = \Phi'x \cdot \Phi^0 u, \qquad x \in \mathbb{C}\mathrm{a}^2, \qquad u \in \mathbb{C}\mathrm{a}^{\oplus}.$$

Hence there is by Proposition 5 of Lecture 15 one and only one element $a \in \mathrm{Spin}(9)$ with the property that $\Phi' = a^R$ and $\Phi^0 = a^T$.

Thus we have associated every automorphism $\Phi \in K$ with some element $a \in \mathrm{Spin}(9)$. It is clear that the mapping obtained is a homomorphism. Moreover, since identity (10) is obviously necessary and sufficient for the corresponding mapping Φ to be an automorphism of the algebra $\mathbb{A}\mathrm{l}$ that

mapping is an isomorphism. We thus see that the *subgroup K is naturally isomorphic to the spinor group* Spin(9).

Identifying via that isomorphism the subgroup K with Spin(9) we finally discover that Spin(9) *is contained in the group F_4, with the corresponding quotient manifold being diffeomorphic to the octave projective plane*:

$$F_4/\mathrm{Spin}(9) \approx \mathbb{C}\mathrm{aP}^2. \tag{11}$$

It follows, in particular, that $\dim F_4 = \dim \mathrm{Spin}(9) + \dim \mathbb{C}\mathrm{aP}^2 = 36 + 16 = 52$.

Now we are ready to prove for F_4 a proposition completely similar to Proposition 1 of Lecture 15 for the group G_2:

Proposition 2. *The group F_4 is connected and simply connected. Every Lie group which is locally isomorphic to F_4 is isomorphic to it.*

Proof. The first statement follows immediately from the existence of diffeomorphism (11), since Spin(9) and projective plane $\mathbb{C}\mathrm{aP}^2$ are connected and simply connected.

To prove the second statement it suffices for us to establish that the centre of F_4 is trivial (i.e. it consists only of an identity automorphism). But if the automorphism Φ_0: $\mathbb{A}\mathrm{l} \to \mathbb{A}\mathrm{l}$ is in the centre of the group F_4, then since not a single idempotent, except E_1, leaves fixed all the elements of the subgroup $K \approx \mathrm{Spin}(9)$ the reasoning we have already used (see the proof of Proposition 1 in Lecture 15) shows that $\Phi_0 \in K$ and so $\Phi_0 = \pm\mathrm{id}$ (for the centre of Spin(9) consists only of elements ± 1). Since $(-E_1)^2 = E_1 \neq -E_1$, the operator $-\mathrm{id}$ is not an automorphism. Therefore $\Phi_0 = \mathrm{id}$. □

Remark 2. If an automorphism Φ: $\mathbb{A}\mathrm{l} \to \mathbb{A}\mathrm{l}$ leaves fixed every idempotent E_i, $i = 1, 2, 3$, then, as is easily seen, it sends every matrix of the form $X_i(\xi)$, $i = 1, 2, 3$, to a matrix $X_i(\xi^{(i)})$, $i = 1, 2, 3$, where $\xi^{(i)}$ is some octave linearly dependent on an octave ξ. Thus we obtain three (obviously orthogonal) operators Φ: $\xi \mapsto \xi^{(i)}$ acting in the vector space $\mathbb{C}\mathrm{a}$, and a direct calculation using formula (20) of Lecture 15 shows that for these operators we have an identity

$$\Phi_1\xi \cdot \Phi_2\eta = \Phi_3(\overline{\overline{\xi}\overline{\eta}}), \quad \xi, \eta \in \mathbb{C}\mathrm{a}.$$

By Proposition 3 of Lecture 15, therefore, there is one and only one element $a \in \mathrm{Spin}(8)$ for which $\Phi_1 = a^L$, $\Phi_2 = a^R$

and $\Phi_3' \circ \sigma = a^T$, where σ: $\xi \mapsto \bar{\xi}$ is a conjugation in the algebra $\mathbb{C}$a. Since the resulting correspondence $\Phi \mapsto a$ is obviously an isomorphism, this proves that the *group* Aut^0 Al *of automorphisms of the algebra* Al *that leave fixed all idempotents* E_i, $i = 1, 2, 3$, *is isomorphic to* Spin(8).

Since the Lie group $F_4 = \mathrm{Aut}$ Al is simply connected, its algebraic structure is completely defined by that of the Lie algebra $\mathfrak{f}_4 = \mathrm{Der}$ Al. It only remains for us to study that Lie algebra.

To this end we select in $\mathfrak{f}_4$ a subalgebra Der^0 Al consisting of differentiations nullifying every idempotent E_i, $i = 1, 2, 3$. That subalgebra is clearly a Lie algebra of the subgroup Aut^0 Al (see Remark 2) and is therefore isomorphic to the Lie algebra $\mathfrak{l}$ (Spin(8)) $\approx \mathfrak{so}(8)$. This isomorphism is easy to establish also directly, though. Indeed, if $DE_i = 0$, $i = 1, 2, 3$, then, as is immediate from formulas (19) of Lecture 15, for any $i = 1, 2, 3$ the element DX_i (ξ) is of the form X_i (A_i, ξ), where A_i is a linear operator $\mathbb{C}\mathrm{a} \to \mathbb{C}\mathrm{a}$. The operators A_i are skew-symmetric and (as is immediate at $i = 1$ from formulas (20) of Lecture 15) satisfy the identity

$$A_1\xi\cdot\eta + \xi\cdot A_2\eta = A_3\,(\overline{\xi\eta}). \tag{12}$$

Therefore (see Remark 2 of Lecture 15) $A_2 = (A_1^{\lambda^{-1}})^{\rho}$ and $A_3 = A_1^{\lambda^{-1}} \circ \sigma$, where σ: $\mathbb{C}\mathrm{a} \to \mathbb{C}\mathrm{a}$ is a conjugation. Since, conversely, any operators A_1, A_2, A_3 which satisfy identity (12) obviously correspond to some differentiation $D \in \mathrm{Der}^0$ Al, this proves that the correspondence $D \mapsto A_1$ is an isomorphism. □

We shall denote a differentiation in Der^0 Al corresponding to an operator $A \in \mathfrak{so}$ (8) by $\varkappa A$. Thus $D = \varkappa A_1$ if and only if $DE_i = 0$ for any $i = 1, 2, 3$ and DX_1 (ξ) $= X_1$ ($A\xi$) for $\xi \in \mathbb{C}$a.

Now let D be a differentiation in Al and let

$$DE_i = a_{1i}E_1 + a_{2i}E_2 + a_{3i}E_3 + X_1(\xi_{1i}) + X_2(\xi_{2i}) + X_3(\xi_{3i}).$$

Since $E_i^2 = E_i$, we have $2DE_i \circ E_i = DE_i$ from which by formulas (18) to (20) of Lecture 15 it follows immediately that $a_{ij} = 0$ for any i, j, and $\xi_{ii} = 0$. Besides, since $E_i \circ E_j = 0$ for $i \neq j$, we have $DE_i \circ E_j + E_i \circ DE_j = 0$, from which it follows that $\xi_{i,\,i+1} + \xi_{i,\,i+2} = 0$ for any $i = 1, 2, 3$.

Hence putting $\xi_i = \xi_{i,\,i+1}$ we get

(13) $DE_i = X_{i+1}(\xi_{i+1}) - X_{i+2}(\xi_{i+2}), \quad i = 1, 2, 3 \bmod 3.$

On the other hand, a direct calculation shows that for an adjoint differentiation $D = \operatorname{ad} A$ corresponding to a matrix $A = Y_1(\xi_1) + Y_2(\xi_2) + Y_3(\xi_3)$ in $\mathbb{M}^0$ we have the same formulas (13). This means that for any differentiation $D \in \operatorname{Der} \mathbb{A}\mathrm{l}$ there is one and only one adjoint differentiation $\operatorname{ad} A$, $A \in \mathbb{M}^0$, with the property that $D - \operatorname{ad} A \in \operatorname{Der}^0 \mathbb{A}\mathrm{l} = \varkappa(\mathfrak{so}(8))$, i.e. that

(14) $$\mathfrak{f}_4 = \varkappa(\mathfrak{so}(8)) \oplus \operatorname{ad} \mathbb{M}^0.$$

Since the mappings $\varkappa\colon \mathfrak{so}(8) \to \mathfrak{f}_4$ and $\operatorname{ad}\colon \mathbb{M}^0 \to \mathfrak{f}_4$ are monomorphisms, this proves that

$$\mathfrak{f}_4 \approx \mathfrak{so}(8) \oplus \mathbb{M}^0.$$

Since $\dim \mathfrak{so}(8) = 28$ and $\dim \mathbb{M}^0 = 24$, this again proves in particular that $\dim \mathfrak{f}_4 = 52$.

In view of decomposition (14), for the structure of $\mathfrak{f}_4$ to be completely defined it suffices to calculate all possible commutators of elements of the form $\varkappa A$ and $\operatorname{ad} Y_i(\xi)$, where $A \in \mathfrak{so}(8)$, $\xi \in \mathbb{C}\mathrm{a}$, $i = 1, 2, 3$. It turns out that

(15) $$[\varkappa A, \varkappa B] = \varkappa[A, B],$$

(16) $$[\varkappa A, \operatorname{ad} Y_i(\xi)] = \operatorname{ad} Y_i(A\xi),$$

(17) $$[\operatorname{ad} Y_i(\xi), \operatorname{ad} Y_j(\eta)] = \begin{cases} \varkappa C^{(i)}_{\xi,\eta}, & \text{if } j = i, \\ \operatorname{ad} Y_{i+2}(-\overline{\xi\eta}), & \text{if } j = i+1, \end{cases}$$

where A and B are elements of $\mathfrak{so}(8)$ (interpreted as skew-symmetric operators $\mathbb{C}\mathrm{a} \to \mathbb{C}\mathrm{a}$), ξ, η are octaves and $C^i_{\xi,\eta}$ are operators $\mathbb{C}\mathrm{a} \to \mathbb{C}\mathrm{a}$ defined respectively by formulas

$$C^{(1)}_{\xi,\eta}\colon \zeta \mapsto 4(\xi, \eta)\eta - 4(\eta, \xi)\xi,$$

$$C^{(2)}_{\xi,\eta}\colon \zeta \mapsto \zeta\xi \cdot \bar\eta - \zeta\eta \cdot \bar\xi, \quad \zeta \in \mathbb{C}a.$$

$$C^{(3)}_{\xi,\eta}\colon \zeta \mapsto \bar\eta \cdot \xi\zeta - \bar\xi \cdot \eta\xi.$$

Indeed formula (15) is equivalent to the statement that the mapping $\varkappa$ is a homomorphism while formulas (16) and (17) can be verified by direct calculation. It is easy to see,

for example, that

$$[Y_1(\xi)\, E_1] = 0,\ [Y_1(\xi), E_2] = -X_1(\xi),\ [Y_1(\xi)\, E_3] = X_1(\xi),$$

i.e. that $(\mathrm{ad}\, Y_1(\xi))\, E_i = \varepsilon_i X_1(\xi)$, where $\varepsilon_i = 0, -1, 1$ for $i = 1, 2, 3$. Therefore (since by definition $(\varkappa A)\, E_i = 0$ for any $i = 1, 2, 3$)

$$\begin{aligned}[\varkappa A,\ \mathrm{ad}\ Y_1(\xi)]\, E_i &= (\varkappa A)\,(\mathrm{ad}\ Y_1(\xi))\, E_i \\ &= \varepsilon_i X_1(A\xi) = (\mathrm{ad}\ Y_1(A\xi))\, E_i\end{aligned}$$

and hence the differentiation $D = [\varkappa A,\ \mathrm{ad}\ Y_1(\xi)] - \mathrm{ad}\ Y_1(A\xi)$ is in $\mathrm{Der}^0\,\mathfrak{A}\mathrm{l}$. As an obvious calculation shows,

$$[Y_1(\xi),\ X_1(\zeta)] = 2\,(\xi,\ \zeta)\,(E_2 - E_3)$$

and hence the formula

$$\begin{aligned}DX_1(\zeta) &= (\varkappa A)\,(2\,(\xi,\ \zeta)\,(E_2 - E_3)) \\ &\quad - [Y_1(\xi),\ X_1(A\zeta)] - [Y_1(A\xi),\ X_1(\zeta)] \\ &= -2\,[(\xi,\ (A\xi) + (A\xi,\ \zeta)]\,(E_2 - E_3) = 0,\end{aligned}$$

holds for D, since by hypothesis the operator A is skew-symmetric. Consequently, $D = 0$, which proves formula (16) for $i = 1$. Similarly

$$\begin{aligned}&[\mathrm{ad}\ Y_1(\xi),\ \mathrm{ad}\ Y_1(\eta)]\, E_i \\ &\quad = \varepsilon_i\,(\mathrm{ad}\, Y_1(\xi))\, X_1(\eta) - \varepsilon_i\,(\mathrm{ad}\, Y_1(\eta))\, X_1(\xi) \\ &\quad = 2\varepsilon_i\,((\xi, \eta) - (\eta,\ \xi))\,(E_2 - E_3) = 0\end{aligned}$$

and

$$\begin{aligned}&[\mathrm{ad}\, Y_1(\xi),\ \mathrm{ad}\, Y_1(\eta)]\, X_1(\zeta) \\ &\quad = 2\,((\eta,\ \zeta)\,\mathrm{ad}\, Y_1(\xi) - (\xi,\ \zeta)\,\mathrm{ad}\, Y_1(\eta))\,(E_2 - E_3) \\ &\quad = 4\,(-(\eta,\ \zeta)\, X_1(\xi) + (\xi,\ \zeta)\, X_1(\eta)),\end{aligned}$$

which proves formula (17) at $i = j = 1$. The remaining formulas (16) and (17) can be verified in exactly the same way. □

The results obtained make it possible to prove for the Lie algebra $\mathfrak{f}_4$ an analogue of Proposition 1 of Lecture 14.

Let $\mathfrak{h}$ be a four-dimensional subspace of $\mathfrak{f}_4$ consisting of linear combinations of elements $\varkappa E_{[1,\,8]}$, $\varkappa E_{[2,\,7]}$, $\varkappa E_{[3,\,6]}$

and $\varkappa E_{[4,\,5]}$. Since these elements commute with one another, we have $[H_1, H_2] = 0$ for any elements $H_1, H_2 \in \mathfrak{h}$. Let e_1, e_2, e_3, e_4 be a basis of the conjugate vector space $\mathfrak{h}^*$ dual to the basis $\varkappa E_{[1,\,8]}, \varkappa E_{[2,\,7]}, \varkappa E_{[3,\,6]}, -\varkappa E_{[4,\,5]}$ of the vector space $\mathfrak{h}$. Introducing into $\mathfrak{h}^*$ a Euclidean structure in which the basis e_1, e_2, e_3, e_4 is orthonormal we give the name of *configuration* $\boldsymbol{F}_4$ to the collection of all possible vectors of the form

$$\pm e_p, \ \pm e_p \pm e_q \qquad (p \neq q),$$
$$\frac{1}{2}(\pm e_1 \pm e_2 \pm e_3 \pm e_4),$$

where any combinations of signs (the number of the vectors is 48) are admissible.

By virtue of the identification $\mathfrak{h}^* = \mathfrak{h}$ induced by the Euclidean structure we may consider vectors $\alpha \in \boldsymbol{F}_4$ as elements in $\mathfrak{h}$. Following the example of the Lie algebra $\mathfrak{g}_4^{\mathbb{C}}$ (see Lecture 14) we put

$$H_\alpha = \frac{2\alpha}{|\alpha|^2} \text{ for any } \alpha \in \boldsymbol{F}_4.$$

Next, denoting the imaginary unit of the field $\mathbb{C}$ by $\sqrt{-1}$ to avoid confusion with an element in $\mathbb{C}a$, we define the elements X_α, $\alpha = \pm e_p \pm e_q$, of the complexified Lie algebra $\mathfrak{f}_4^{\mathbb{C}} = \mathfrak{f}_4 \otimes \mathbb{C}$ by setting

$$X_{e_1 \pm e_2} = \varkappa(E_{[7,\,8]} \pm E_{[1,\,2]}) + \sqrt{-1}\cdot\varkappa(E_{[7,\,1]} \pm E_{[2,\,8]}),$$
$$X_{-e_1 \pm e_2} = \varkappa(-E_{[7,\,8]} \pm E_{[1,\,2]}) + \sqrt{-1}\cdot\varkappa(E_{[7,\,1]} \mp E_{[2,\,8]})$$

and assuming that the other vectors $X_{\pm e_p \pm e_q}$ are given by the formulas resulting from replacing the indices (7, 8) by (2, 7), (3, 6), (5, 4) when p is equal to 2, 3, 4 and, respectively, the indices (1, 2) by (1, 8), (3, 6), (5, 4) when q is equal to 1, 3, 4.

For $\alpha = \pm e_p$ we set

$$X_{\pm e_p} = \operatorname{ad} Y_1(\xi_p) \pm \sqrt{-1}\operatorname{ad} Y_1(\eta_p),$$

where

$$\xi_1 = 1, \qquad \xi_2 = i, \qquad \xi_3 = j, \qquad \xi_4 = k,$$
$$\xi_1 = -h, \qquad \eta_2 = -g, \qquad \eta_3 = -f, \qquad \eta_4 = -e,$$

$e_1 \pm e_2 \pm e_3 \pm e_4)$ we set

$$\text{ad}\, Y_2(\xi_p) + \sqrt{-1}\,\text{ad}\, Y_2(\eta_p),$$
$$\text{ad}\, Y_3(\xi_3) + \sqrt{-1}\,\text{ad}\, Y_3(\eta_p),$$

$$\pm\frac{1}{2}(-e_1+e_2+e_3+e_4),$$
$$\pm\frac{1}{2}(-e_1+e_2-e_3-e_4),$$
$$\pm\frac{1}{2}(-e_1-e_2+e_3-e_4),$$
$$\pm\frac{1}{2}(-e_1-e_2-e_3+e_4),$$

$$\pm\frac{1}{2}(-e_1-e_2-e_3-e_4),$$
$$\pm\frac{1}{2}(e_1+e_2-e_3-e_4),$$
$$\pm\frac{1}{2}(e_1-e_2+e_3-e_4),$$
$$\pm\frac{1}{2}(e_1-e_2-e_3+e_4),$$

ber of the corresponding vector α in these

; that *Proposition* 1 *of Lecture* 14 (*together f the lecture*) *will hold also for the algebra* ı the configuration F_4, of course).

can be proved by choosing in $\mathfrak{f}_4^{\mathbb{C}}$ an nd repeating step by step the calculations n 1 and formula (17) for the Lie algebra ınt of work required will now be sub- lext semester we shall develop a general is work to be reduced, and therefore we or the time being.

een said it is not surprising that *there is* ' *Propositions* 2 *of Lecture* 14 *holding for*

$\mathfrak{f}_4^{\mathbb{C}}$. To obtain a formulation of that proposition for $\mathfrak{f}_4^{\mathbb{C}}$ it suffices to assume in formulas (23) of Lecture 14 that the indices p and q change from 1 to 4 and the numbers n_{pq} are elements of the matrix

$$\begin{pmatrix} 2 & -1 & 0 & 0 \\ -1 & 2 & -2 & 0 \\ 0 & -1 & 2 & -1 \\ 0 & 0 & -1 & 2 \end{pmatrix}.$$

This statement can be proved using the same considerations but, of course, it requires much more work to be done. The role of vectors $\boldsymbol{f}_1$, $\boldsymbol{e}_2$ will be played by vectors

$$\frac{1}{2}(\boldsymbol{e}_1-\boldsymbol{e}_2-\boldsymbol{e}_3-\boldsymbol{e}_4), \quad \boldsymbol{e}_4, \quad \boldsymbol{e}_3-\boldsymbol{e}_4, \quad \boldsymbol{e}_2-\boldsymbol{e}_3.$$

The details of the calculations will be left to the reader.

Lecture 17

Solvable Lie algebras · The radical of a Lie algebra · Abelian Lie algebras · The centre of a Lie algebra · Nilpotent Lie algebras · The nilradical of a Lie algebra · Linear Lie nilalgebras · The Engel theorem · Criteria of nilpotency · Linear irreducible Lie algebras. Reductive Lie algebras · Linear solvable Lie algebras · The nilpotent radical of a Lie algebra

We now turn to the general theory of Lie algebras so as to prove the Ado theorem and thus fill in the remaining gap in the proof of the Cartan theorem in Lecture 10.

The proof of the Ado theorem is based on a rather advanced structural theory of Lie algebras that is of independent interest. Unfortunately, we shall be able to touch only in a very perfunctory way upon this theory.

Unless otherwise specified, in what follows a ground field $\mathbb{K}$ is taken to be a field of characteristic 0. All Lie algebras over $\mathbb{K}$ are assumed finite-dimensional.

Let $\mathfrak{g}$ be a Lie algebra over $\mathbb{K}$. For any two subspaces $\mathfrak{a}$ and $\mathfrak{b}$ of $\mathfrak{g}$ we denote by $[\mathfrak{a}, \mathfrak{b}]$ a subspace generated by elements of the form $[a, b]$ where $a \in \mathfrak{a}$, $b \in \mathfrak{b}$. In this notation the property for the subspace $\mathfrak{a}$ of being a subalgebra is equivalent to the inclusion $[\mathfrak{a}, \mathfrak{a}] \subset \mathfrak{a}$ and the property of being an ideal is equivalent to the inclusion $[\mathfrak{a}, \mathfrak{g}] \subset \mathfrak{a}$. Since by the Jacobi identity $[[\mathfrak{a}, \mathfrak{b}], \mathfrak{c}] \subset [[\mathfrak{b}, \mathfrak{c}], \mathfrak{a}] + [[\mathfrak{c}, \mathfrak{a}], \mathfrak{b}]$ it follows in particular that *if* $\mathfrak{a}$ *and* $\mathfrak{b}$ *are ideals, then* $[\mathfrak{a}, \mathfrak{b}]$ *is also an ideal.*

Therefore formulas

$$\mathfrak{g}^{(1)} = \mathfrak{g}, \quad \mathfrak{g}^{(2)} = [\mathfrak{g}, \mathfrak{g}], \ \ldots, \ \mathfrak{g}^{(k)} = [\mathfrak{g}^{(k-1)}, \ \mathfrak{g}^{(k-1)}], \ \ldots$$

define in $\mathfrak{g}$ a descending (more precisely, nonascending) chain of ideals

$$\mathfrak{g} = \mathfrak{g}^{(1)} \supset \mathfrak{g}^{(2)} \ldots \mathfrak{g}^{(k)} \supset \ldots$$

Note that $\mathfrak{g}^{(k)(l)} = \mathfrak{g}^{(k+l-1)}$.

The ideal $\mathfrak{g}^{(k)}$ is also symbolized $\mathfrak{g}^{(k-1)}$ by some mathematicians.

Definition 1. A Lie algebra $\mathfrak{g}$ is said to be *solvable* if there is $k \geqslant 0$ such that $\mathfrak{g}^{(k)} = 0$.

Let $n = \dim \mathfrak{g}$. A descending chain of subspaces

$$\mathfrak{g} = \mathfrak{g}_0 \supset \mathfrak{g}_1 \ldots \supset \mathfrak{g}_i \supset \ldots \supset \mathfrak{g}_n = 0$$

is said to be a *flag* if the dimension of every subspace is a unity smaller than that of the preceding subspace, i.e. if $\dim \mathfrak{g}_i = n - i$ for any $i = 0, 1, \ldots, n$. A flag consisting of subalgebras is called a *flag of subalgebras*.

Proposition 1. *A Lie algebra $\mathfrak{g}$ is solvable if and only if it has a flag of subalgebras*

$$\mathfrak{g} = \mathfrak{g}_0 \supset \mathfrak{g}_1 \supset \ldots \supset \mathfrak{g}_i \ldots \supset \mathfrak{g}_n = 0,$$

in which every subalgebra $\mathfrak{g}_i$, $i = 1, \ldots, n$, is an ideal of the preceding subalgebra $\mathfrak{g}_{i-1}$ (satisfies the relation $[\mathfrak{g}_{i-1}, \mathfrak{g}_i] \subset \mathfrak{g}_i$).

Proof. By hypothesis $\dim \mathfrak{g}_{i-1} = \dim \mathfrak{g}_i + 1$. Therefore any element in $\mathfrak{g}_{i-1}$ is of the form $x + \lambda e$, where $x \in \mathfrak{g}_i$, $\lambda \in \mathbb{K}$ and e is a fixed element. Since

$$[x + \lambda e, y + \mu e] = [x, y] + \lambda [x, e] - \mu [y, e]$$

and $[x, y]$, $[x, e]$, $[y, e] \in \mathfrak{g}_i$ (for $\mathfrak{g}_i$ is an ideal in $\mathfrak{g}_{i-1}$), it follows that $[\mathfrak{g}_{i-1}, \mathfrak{g}_{i-1}] \subset \mathfrak{g}_i$. Hence if $\mathfrak{g}^{(i)} \subset \mathfrak{g}_{i-1}$, then $\mathfrak{g}^{(i+1)} = [\mathfrak{g}^{(i)}, \mathfrak{g}^{(i)}] \subset [\mathfrak{g}_{i-1}, \mathfrak{g}_{i-1}] \subset \mathfrak{g}_i$. Since the inclusion $\mathfrak{g}^{(i)} \subset \mathfrak{g}_{i-1}$ is true for $i = 1$, it is thus proved for all $i = 1, \ldots, n + 1$. In particular, $\mathfrak{g}^{(n+1)} \subset \mathfrak{g}_n = 0$, i.e. $\mathfrak{g}^{(n+1)} = 0$.

Conversely, if there is $k \geqslant 0$ such that $\mathfrak{g}^{(k)} = 0$ (and $\mathfrak{g}^{(k-1)} \neq 0$), then in the chain of ideals

$$\mathfrak{g} = \mathfrak{g}^{(0)} \supset \mathfrak{g}^{(1)} \supset \ldots \supset \mathfrak{g}^{(k)} = 0$$

the inclusions are all strict and therefore that chain can be embedded into some flag

$$\mathfrak{g} = \mathfrak{g}_0 \supset \mathfrak{g}_1 \ldots \supset \mathfrak{g}_n = 0,$$

Let $i = 0, 1, \ldots, n$, and let a be the greatest index for which $\mathfrak{g}_i \subset \mathfrak{g}^{(a)}$. If $\mathfrak{g}_i \neq \mathfrak{g}^{(a)}$, then $\mathfrak{g}_{i-1} \subset \mathfrak{g}^{(a)}$ and so $[\mathfrak{g}_{i-1}, \mathfrak{g}_i] \subset [\mathfrak{g}^{(a)}, \mathfrak{g}^{(a)}] = \mathfrak{g}^{(a+1)} \subset \mathfrak{g}_i$. If, however, $\mathfrak{g}_i = \mathfrak{g}^{(a)}$, then $\mathfrak{g}_{i-1} \subset \mathfrak{g}^{(a-1)}$ and so $[\mathfrak{g}_{i-1}, \mathfrak{g}_i] \subset [\mathfrak{g}^{(a-1)}, \mathfrak{g}^{(a)}] \subset \mathfrak{g}^{(a)} = \mathfrak{g}_i$. Thus in all the cases $[\mathfrak{g}_{i-1}, \mathfrak{g}_i] \subset \mathfrak{g}_i$, from which it follows that the flag under consideration is a flag of subalgebras (because $[\mathfrak{g}_i, \mathfrak{g}_i] \subset [\mathfrak{g}_{i-1}, \mathfrak{g}_i] \subset \mathfrak{g}_i$) in which every subalgebra is an ideal of the previous algebra. □

Under any epimorphism $\mathfrak{g} \to \mathfrak{h}$ ideals $\mathfrak{g}^{(k)}$ obviously go over into ideals $\mathfrak{h}^{(k)}$. Similarly, if $\mathfrak{h} \subset \mathfrak{g}$, then $\mathfrak{h}^{(k)} \subset \mathfrak{g}^{(k)} \cap \mathfrak{h}$. Therefore *every quotient algebra and every subalgebra of a solvable Lie algebra is solvable.* Besides, it is easy to see that $\mathfrak{g}$ *is a solvable algebra if it contains a solvable ideal* $\mathfrak{h}$ *for which the quotient algebra* $\mathfrak{g}/\mathfrak{h}$ *mod is solvable.* Indeed, if $(\mathfrak{g}/\mathfrak{h})^{(k)} = 0$, then $\mathfrak{g}^{(k)} = \mathfrak{h}$ and hence if $\mathfrak{h}^{(l)} = 0$, then $\mathfrak{g}^{(k+l-1)} = \mathfrak{g}^{(k)(l)} = 0$. □

For any two ideals $\mathfrak{a}$ and $\mathfrak{b}$ their sum $\mathfrak{a} + \mathfrak{b}$ is also an ideal, the quotient algebra $(\mathfrak{a} + \mathfrak{b})/\mathfrak{b}$ being (by the so-called first theorem on isomorphisms) isomorphic to $\mathfrak{a}/\mathfrak{a} \cap \mathfrak{b}$ and therefore solvable if the ideal $\mathfrak{a}$ is solvable. Consequently, if the ideal $\mathfrak{b}$ is also solvable, so is the ideal $\mathfrak{a} + \mathfrak{b}$. Thus the *sum* $\mathfrak{a} + \mathfrak{b}$ *of two solvable ideals* $\mathfrak{a}$ *and* $\mathfrak{b}$ *is a solvable ideal. In any finite-dimensional Lie algebra* $\mathfrak{g}$ *therefore there is a largest solvable ideal* $\mathfrak{r}$ containing all solvable ideals of that algebra: it is the sum of all solvable ideals of $\mathfrak{g}$.

Definition 2. The ideal $\mathfrak{r}$ is called the *radical* of a Lie algebra $\mathfrak{g}$. If $\mathfrak{r} = 0$, the Lie algebra is called *semisimple algebra.*

Note that any homomorphism $\mathfrak{g} \to \mathfrak{h}$ maps the radical of $\mathfrak{g}$ into the radical of $\mathfrak{h}$.

The natural epimorphism $\mathfrak{g} \to \mathfrak{g}/\mathfrak{r}$ sets up a bijective correspondence between ideals $\mathfrak{a}$ of $\mathfrak{g}$ which contains an ideal $\mathfrak{r}$ and ideals $\mathfrak{b}$ of the algebra $\mathfrak{g}/\mathfrak{r}$. An ideal $\mathfrak{b}$ corresponding to an ideal $\mathfrak{a}$ is isomorphic to the quotient algebra $\mathfrak{a}/\mathfrak{r}$ and hence solvable if and only if the ideal $\mathfrak{a}$ is solvable. By the maximality of the radical $\mathfrak{r}$ the ideal $\mathfrak{a} \supset \mathfrak{r}$ is solvable if and only if $\mathfrak{a} = \mathfrak{r}$. This proves that there are no nonzero solvable ideals in the quotient algebra $\mathfrak{g}/\mathfrak{r}$, i.e. $\mathfrak{g}/\mathfrak{r}$ *is semisimple algebra.*

Definition 3. A Lie algebra $\mathfrak{g}$ is said to be *Abelian* if $\mathfrak{g}^{(2)} = 0$, i.e. if $[x, y] = 0$ for any elements $x, y \in \mathfrak{g}$.

If a Lie algebra $\mathfrak{g}$ is not semisimple, i.e. if its radical $\mathfrak{r}$ is nonzero, and if k is the smallest exponent for which $\mathfrak{r}^{(k)} = 0$, then the ideal $\mathfrak{a} = \mathfrak{r}^{(k-1)}$ (which is obviously an ideal in $\mathfrak{g}$ as well) is nonzero and Abelian ($[\mathfrak{a}, \mathfrak{a}] = [\mathfrak{r}^{(k-1)}, \mathfrak{r}^{(k-1)}] = \mathfrak{r}^{(k)} = 0$). Conversely, if in a Lie algebra $\mathfrak{g}$ there is an Abelian ideal $\mathfrak{a} \neq 0$ (which is consequently solvable) then $\mathfrak{r} \neq 0$ and hence $\mathfrak{g}$ is not semisimple. Thus a *Lie algebra $\mathfrak{g}$ is semisimple if and only if there are no nonzero Abelian ideals in it.*

The *centre* of a Lie algebra $\mathfrak{g}$ is its annulet in the sense of the general theory of algebras, i.e. the largest subspace $\mathfrak{z} \subset \mathfrak{g}$ for which $[\mathfrak{z}, \mathfrak{g}] = 0$. It can be verified in an obvious way that the *centre is an ideal.*

An algebra $\mathfrak{g}$ is Abelian if and only if $\mathfrak{z} = \mathfrak{g}$.

Since a centre is an Abelian ideal, the *centre of a semisimple algebra is zero.*

Along with the ideals $\mathfrak{g}^{(k)}$ one can also consider ideals $\mathfrak{g}^{(k)}$ defined by induction using the formula

$$\mathfrak{g}^k = [\mathfrak{g}, \mathfrak{g}^{k-1}], \qquad (\mathfrak{g}^1 = \mathfrak{g}).$$

Note that $\mathfrak{g}^2 = \mathfrak{g}^{(2)}$.

Definition 4. A Lie algebra $\mathfrak{g}$ is said to be *nilpotent* if there is $k \geqslant 1$ such that $\mathfrak{g}^k = 0$.

Since $\mathfrak{g}^2 = \mathfrak{g}^{(2)}$ we see in particular that *any Abelian Lie algebra is nilpotent.*

By induction on i we immediately find that $\mathfrak{g}^{(i)} \subset \mathfrak{g}^i$ for any i. Therefore *any nilpotent Lie algebra is solvable.*

If $\mathfrak{g}^k = 0$ and $\mathfrak{g}^{k-1} \neq 0$, then the nonzero ideal $\mathfrak{a} = \mathfrak{g}^{k-1}$ has the property that $[\mathfrak{a}, \mathfrak{g}] = 0$ and therefore is in the centre $\mathfrak{z}$ of the algebra $\mathfrak{g}$. Hence the *centre $\mathfrak{z}$ of a nilpotent Lie algebra is nonzero.*

Note that the centre of a solvable Lie algebra may well be zero.

Proposition 2. *A Lie algebra $\mathfrak{g}$ is nilpotent if and only if there is a flag of subalgebras*

$$\mathfrak{g} = \mathfrak{g}_0 \supset \mathfrak{g}_1 \supset \ldots \supset \mathfrak{g}_i \supset \ldots \supset \mathfrak{g}_n = 0,$$

in it, such that for any $i = 1, \ldots, n$ there is an inclusion $[\mathfrak{g}, \mathfrak{g}_{i-1}] \subset \mathfrak{g}_i$ (so that, in particular, every subalgebra $\mathfrak{g}_{i-1}$ is an ideal of $\mathfrak{g}$).

Proof. (Cf. the proof of Proposition 1.) If $\mathfrak{g}^i \subset \mathfrak{g}_{i-1}$, then $\mathfrak{g}^{i+1} = [\mathfrak{g}, \mathfrak{g}^i] \subset [\mathfrak{g}, \mathfrak{g}_{i-1}] \subset \mathfrak{g}_i$. Since $\mathfrak{g}^1 = \mathfrak{g}_0$, this proves by induction that $\mathfrak{g}^i \subset \mathfrak{g}_{i-1}$ for any $i = 1, \ldots, n$. In particular, $\mathfrak{g}^{n+1} \subset \mathfrak{g}_n = 0$ and hence $\mathfrak{g}^{n+1} = 0$.

Conversely, if there is $k \geqslant 1$ such that $\mathfrak{g}^k = 0$, then (provided $\mathfrak{g}^{k-1} \neq 0$) all inclusions in the chain of ideals

$$\mathfrak{g} = \mathfrak{g}^1 \supset \mathfrak{g}^2 \supset \ldots \supset \mathfrak{g}^k = 0$$

are strict and so the chain can be embedded into the flag of subspaces

$$\mathfrak{g} = \mathfrak{g}_0 \supset \mathfrak{g}_1 \supset \ldots \supset \mathfrak{g}_n = 0.$$

If now a is the largest index for which $\mathfrak{g}_i \subset \mathfrak{g}^a$, then $\mathfrak{g}^{a+1} \subset \mathfrak{g}_{i+1}$ and therefore

$$[\mathfrak{g}, \mathfrak{g}_i] \subset [\mathfrak{g}, \mathfrak{g}^a] = \mathfrak{g}^{a+1} \subset \mathfrak{g}_{i+1}. \quad \square$$

It can be proved, just as for the case of solvable algebras, that *any subalgebra and any quotient algebra of a nilpotent algebra are nilpotent algebras*. The corresponding statement for extensions is in general false, however. One may only say that *a Lie algebra* $\mathfrak{g}$ *is nilpotent if so is its quotient algebra* $\mathfrak{g}/\mathfrak{h}$ mod *some ideal* $\mathfrak{h}$ *which is contained in its centre* $\mathfrak{z}$. Indeed, if $(\mathfrak{g}/\mathfrak{h})^k = 0$, then $\mathfrak{g}^k \subset \mathfrak{h} \subset \mathfrak{z}$ and so $\mathfrak{g}^{k+1} = [\mathfrak{g}, \mathfrak{g}^k] \subset [\mathfrak{g}, \mathfrak{z}] = 0$. $\square$

For every ideal $\mathfrak{a}$ of a Lie algebra $\mathfrak{g}$ its ideals $\mathfrak{a}^k$ are obviously ideals in $\mathfrak{g}$ as well. More generally, if we consider two ideals $\mathfrak{a}$ and $\mathfrak{h}$, then all subspaces

$$\mathfrak{c}_0 = \mathfrak{d}_0, \quad \mathfrak{c}_1 = [\mathfrak{c}_0, \mathfrak{d}_1], \quad \ldots, \quad \mathfrak{c}_i = [\mathfrak{c}_{i-1}, \mathfrak{d}_i],$$

where $\mathfrak{d}_0, \mathfrak{d}_1, \ldots, \mathfrak{d}_i, \ldots$ are ideals, each coinciding with either $\mathfrak{a}$ or $\mathfrak{b}$, will also be ideals in $\mathfrak{g}$. It is easy to see that *for any* $k \geqslant 0$ *there is an inclusion*

$$\mathfrak{c}_k \subset \mathfrak{a}^l,$$

where l *is the number of indices* $i \leqslant k$ *such that* $\mathfrak{d}_i = \mathfrak{a}$. Indeed, for $k = 0$ that inclusion is obviously true (we agree to assume that $\mathfrak{a}^0 = \mathfrak{g}$) and if it is true for some k, then $\mathfrak{c}_{k+1} = [\mathfrak{c}_k, \mathfrak{d}_k] \subset [\mathfrak{a}^l, \mathfrak{d}_k]$ and therefore $\mathfrak{c}_{k+1} \subset \mathfrak{a}^l$ if $\mathfrak{d}_k = \mathfrak{b}$ and $\mathfrak{c}_{k+1} \subset \mathfrak{a}^{l+1}$ if $\mathfrak{d}_{k+1} = \mathfrak{a}$. $\square$

By symmetry there is, of course, also an inclusion $\mathfrak{c}_k \subset \mathfrak{b}^m$ where m is the number of indices $i \leqslant k$ such that $\mathfrak{d}_i = \mathfrak{b}$.

Clearly, either l or m is at least $p = [k/2]$. Therefore either $\mathfrak{c}_k \subset \mathfrak{a}^p$ or $\mathfrak{c}_k \subset \mathfrak{b}^p$, i.e.

$$\mathfrak{c}_k \subset \mathfrak{a}^p \cup \mathfrak{b}^p.$$

On the other hand, it is clear that the ideal $(\mathfrak{a} + \mathfrak{b})^k$ is the sum of ideals of the form $\mathfrak{c}_k$ which correspond to all possible sequences $\mathfrak{d}_0, \mathfrak{d}_1, \ldots, \mathfrak{d}_k$ of ideals $\mathfrak{a}$ and $\mathfrak{b}$. For that ideal therefore there is an inclusion

$$(\mathfrak{a} + \mathfrak{b})^k \subset \mathfrak{a}^p \cup \mathfrak{b}^p.$$

It follows immediately in particular that as with solvable ideals, the *sum* $\mathfrak{a} + \mathfrak{b}$ *of nilpotent ideals* $\mathfrak{a}$ *and* $\mathfrak{b}$ *is a nilpotent ideal. In any Lie algebra* $\mathfrak{g}$ therefore *there is a largest nilpotent ideal* $\mathfrak{n}$ containing all nilpotent ideals of the algebra. That ideal is called the *nilradical* of the Lie algebra $\mathfrak{g}$.

Note that in contrast to the case of the radical the quotient algebra $\mathfrak{g}/\mathfrak{n}$ of a Lie algebra $\mathfrak{g}$ mod its nilradical $\mathfrak{n}$ may well have a nonzero nilradical.

For subalgebras of the commutator algebra $[\mathcal{A}]$ of an arbitrary (in general, finite-dimensional) associative algebra $\mathcal{A}$ and, in particular, for *linear Lie algebras* (subalgebras of the commutator algebra $[\operatorname{End} \mathcal{V}]$ of linear operators acting in some vector space $\mathcal{V}$) one can indicate a very useful sufficient condition for their nilpotency.

Recall that a *linear operator* acting in a vector space $\mathcal{V}$ (or, more generally, an element of an associative algebra $\mathcal{A}$ is said to be *nilpotent* if certain degree of it is zero (see II, 15). Similarly, a *set of linear operators* (or elements of an associative algebra $\mathcal{A}$) is said to be *nilpotent* if there is $k \geqslant 1$ such that the product of any k elements of that set is zero.

We shall apply the latter term to subsets which are subspaces (and, in particular, subalgebras) of $[\mathcal{A}]$ and so, to avoid terminological confusion, subspaces nilpoint in this sense will be called *associatively nilpotent* subspaces (subalgebras). Besides, in accordance with the general terminology accepted in the theory of associative algebras, subalgebras $\mathfrak{g} \subset [\mathcal{A}]$ consisting of nilpotent elements will be called *Lie nilsubalgebras.* Any associatively nilpotent Lie subalgebra is clearly a nilsubalgebra. It is remarkable that the converse is also true:

Proposition 3. *Any finite-dimensional Lie nilsubalgebra* $\mathfrak{g}$ *is associatively nilpotent.*

We shall prove even a more general statement.

Proposition 3* (Jacobson theorem). *Let* $\mathcal{A}$ *be an associative algebra* (not improbable that it is infinite-dimensional) *and let* $\mathcal{Q}$ *be its finite-dimensional subspace generated by some subset* $\mathfrak{g}$ *closed under commutation. If every element* $a \in \mathfrak{g}$ *is nilpotent, then* $\mathcal{Q}$ *is associatively nilpotent.*

Proof. It is easy to see that there are associatively nilpotent subsets (the null set, for example) in $\mathfrak{g}$. Since the rank of the set $\mathfrak{g}$ is finite by hypothesis, there are also maximal associatively nilpotent subsets $\mathfrak{h}$ in it. Since a subspace generated by an associatively nilpotent subset is easily seen to be also associatively nilpotent, it suffices to prove that $\mathfrak{h} = \mathfrak{g}$. Let us assume that $\mathfrak{h} \neq \mathfrak{g}$ and arrive at a contradiction.

Let $\mathcal{P}$ be the span of a maximal associatively nilpotent subset $\mathfrak{h}$ and let p be a number such that the product of any p elements in $\mathcal{P}$ is zero. Then *commuting successively any element* $a \in \mathfrak{g}$ *with any* $2p - 1$ *elements in* $\mathcal{P}$ *results in zero.* Indeed, commuting a with elements $b_1, \ldots, b_{2p-1}$ of $\mathcal{P}$ we ultimately obtain an algebraic sum of products of the form bac, where b is the product of some of the elements $b_1, \ldots, b_{2p-1}$ and c is the product of the rest of these elements. It is clear that either b or c contains at least p factors $b_1, \ldots, b_{2p-1}$ and therefore that product is zero. Consequently all elements of the form bac are zero and hence so is their sum.

It is now clear that *for any element* $a \in \mathfrak{g}$ *there is a number* $s \geqslant 0$ *such that the result of successively commuting it with any* s *elements in* $\mathfrak{h}$ *is in* $\mathcal{P}$, with $s \leqslant 2p - 1$.

It follows that *if* $\mathfrak{h} \neq \mathfrak{g}$, *then there is an element* $a_0 \notin \mathfrak{h}$ *such that* $[a_0, b] \in \mathcal{P}$ *for any* $b \in \mathcal{P}$. For this to be proved it suffices to choose an element $a \in \mathfrak{g} \setminus \mathfrak{h}$ and apply to it the statement proved, noticing that if s is chosen to be the smallest, then there are elements $b_1, \ldots, b_{s-1}$ in $\mathfrak{h}$ such that the result a_0 (which is in $\mathfrak{g}$) of a successive commutation of a with $b_1, \ldots, b_{s-1}$ is not in $\mathfrak{h}$ but has the property that $[a_0, b] \in \mathcal{P}$ for any $b \in \mathfrak{h}$ and hence also for any $b \in \mathcal{P}$.

A *monomial* is the product of elements in $\mathcal{P}$ alternated by the element a_0 (any number in any order). Let r be the number of factors of a monomial a that are in $\mathcal{P}$. It turns

out that *if* $r \geqslant p$, *then* $a = 0$. Indeed, suppose that there is a factor of the form ba_0 in a, with $b \in \mathscr{P}$. Since $[a_0, b] \in \mathscr{P}$, replacing ba_0 by $a_0b - [a_0, b]$ we represent a as a sum of two monomials with the same r. The number of factors of the form a_0 in the first monomial will be by one less and in the second monomial such a factor will be shifted one position left. On repeating this transformation a required number of times we represent a as a sum of monomials which either have no factors of the form a_0 at all or have all these factors collected at the left. Every such monomial is obtained by multiplying an element of the algebra $\mathscr{A}$ by an element that is a product of $r \geqslant p$ elements in $\mathscr{P}$ and is therefore zero. Hence so is the original monomial a.

Since $a_0 \in \mathfrak{g}$, there is by hypothesis an exponent k_0 such that $a_0^{k_0} = 0$. Therefore a monomial a can be nonzero only when exponents of a_0 are smaller than k_0. These degrees are alternated by factors in $\mathscr{P}$ and so their number is not larger than the number r of those factors. Since according to the foregoing for $a \neq 0$ it is necessary that $r < p$, the general number of factors of any nonzero monomial a is at most

$$r - 1 + r(k_0 - 1) \leqslant p - 1 + p(k_0 - 1) = pk_0 - 1.$$

This proves that *if the number of all factors of a monomial a is at least* pk_0, *then* $a = 0$.

In particular this means that so is the product of any pk_0 elements of the set $\bar{\mathfrak{h}} = \{\mathfrak{h}, a_0\}$, i.e. that that set is associatively nilpotent. This contradicts the maximality of the set $\mathfrak{h}$, which completes the proof of Proposition 3*. □

Corollary 1. *Every finite-dimensional Lie nilsubalgebra* $\mathfrak{g} \subset [\mathscr{A}]$ *is nilpotent.*

Proof. Every element of an ideal $\mathfrak{g}^k$ is a linear combination of k-fold commutators of the form

$$x_1, [x_2, \ldots, [x_{k-1}, x_k] \ldots]], \quad x_1, x_2, \ldots, x_k \in \mathfrak{g}$$

and hence (as an element of an algebra $\mathscr{A}$) an algebraic sum of all possible products of the form $x_i^1 \ldots x_i^k$. Consequently, if the Lie algebra $\mathfrak{g}$ is associatively nilpotent, then $\mathfrak{g}^k = 0$ for a sufficiently large k, i.e. that algebra is nilpotent. For the proof to be completed therefore it remains to use Proposition 3. □

In general, this sufficient condition for subalgebras of commutator Lie algebras (and linear Lie algebras, in particular) to be nilpotent *is not necessary*. It is easy to see, for example, that the collection of all matrices of the form $\lambda E + A$, where $A = (a_{ij})$ is a strict upper triangular matrix (i.e. such that $a_{ij} = 0$ for $i \leqslant j$), is a nilpotent subalgebra of a Lie algebra $[\mathbb{R}(n)]$ and at the same time the matrix $\lambda E + A$ is nilpotent only for $\lambda = 0$.

We now return to arbitrary (but as ever finite-dimensional) Lie algebras.

Defined for such an algebra $\mathfrak{g}$ is its homomorphism ad into the commutator algebra of the algebra of all linear operators $\mathfrak{g} \to \mathfrak{g}$ (see Lecture 3). By definition, for any element $a \in \mathfrak{g}$ the linear operator ad a: $\mathfrak{g} \to \mathfrak{g}$ sends any element $x \in \mathfrak{g}$ to an element $[a, x]$. Therefore, in particular, any k-fold commutator $[x_1, [x_2, \ldots, [x_{k-1}, x_k] \ldots]]$ is nothing than the result of applying a linear operator ad $x_1 \circ$ ad $x_2 \circ \ldots$ ad x_{k-1} to the element x_k. This means that a *Lie algebra* $\mathfrak{g}$ *is nilpotent if and only if the linear Lie algebra* ad $\mathfrak{g}$ *is associatively nilpotent*. By virtue of Proposition 3 this proves Corollary 2.

Corollary 2. *A Lie algebra $\mathfrak{g}$ is nilpotent if and only if for any element $a \in \mathfrak{g}$ the linear operator* ad a *is nilpotent.* $\square$

This corollary is known as the *Engel theorem*. However, it is very often Corollary 1 or even Proposition 3 itself that are referred to as the Engel theorem.

Becoming of particular importance in connection with the Engel theorem are the various criteria of nilpotency of a linear operator. Now we prove the first two criteria of this kind.

Recall that a *trace* of a linear operator $\mathcal{A}$ acting in a vector space $\mathscr{V}$ is the sum of diagonal elements of its matrix in a basis of $\mathscr{V}$. The trace is defined correctly (i.e. it is independent of the basis) and symbolized $\operatorname{Tr} A$.

The properties of a trace.

1°. The number $\operatorname{Tr} A$ is linearly dependent on the operator A (i.e. it is a linear functional on the space End $\mathscr{V}$ of all linear operators $\mathscr{V} \to \mathscr{V}$).

2°. For any two operators A and B

$$\operatorname{Tr} AB = \operatorname{Tr} BA.$$

3°. The trace is the sum of all characteristic roots of the operator A (repeated as many times as is their multiplicity):

$$\mathrm{Tr}\, A = \lambda_1 + \ldots + \lambda_n.$$

Property 1° is obvious. Property 2° can be proved by a direct computation, while the easiest way to prove Property 3° is by considering the normal Jordan form of the operator A. (Notice that in Property 3° we go over to the algebraic closure of the field $\mathbb{K}$, i.e. to the field $\mathbb{C}$ when $\mathbb{K} = \mathbb{R}$, but the trace of the operator remains unchanged when the ground field is extended since so does its matrix.)

Since for a nilpotent operator all characteristic roots are zero (see II, 15), it follows from 3° in particular that the *trace of any nilpotent operator is zero.*

This necessary condition for nilpotency is not sufficent, of course. However, since any degree of a nilpotent operator is also a nilpotent operator, it follows that *if an operator A is nilpotent, then* $\mathrm{Tr}\, A^k = 0$ *for any k.*

It turns out that this condition is now not only necessary but also sufficient, i.e. *if* $\mathrm{Tr}\, A^k = 0$ *for any k, then the operator A is nilpotent.* Indeed, since characteristic roots of the operator A^k are the degrees $\lambda_1^k, \ldots, \lambda_n^k$ of the characteristic roots of the operator A, there is, for the trace $\mathrm{Tr}\, A^k$ of the operator A^k, a formula

$$\mathrm{Tr}\, A^k = \lambda_1^k + \ldots + \lambda_n^k,$$

saying that the number $\mathrm{Tr}\, A^k$ is the sum of the kth degrees of the characteristic polynomial of the operator A. But it is known from the theory of polynomials that the coefficients of any polynomial can be polynomially expressed in terms of the sums of degrees of its roots (these are the so-called *Waring formulas*) and are zero if all those sums are zero. As applied to the characteristic polynomial $f_A(\lambda)$ of the operator A, this proves that if $\mathrm{Tr}\, A^k = 0$ for all k, then $f_A(\lambda) = \lambda^n$. Therefore by the Hamilton-Cayley theorem (see II, 16) $A^n = 0$. □

Another, more special sufficient condition for nilpotency relates to operators of the form

$$A = [B_1, C_1] + \ldots + [B_s, C_s] \tag{1}$$

which are commutator sums. It turns out that if an *operator A of the form* (1) *is commutative with each of the operators $B_1, \ldots, B_s$ (i.e. $[A, B_1] = 0, \ldots, [A, B_s] = 0$), then that operator is nilpotent.* Indeed, for any k the operator A^k is also a commutator sum:

$$\begin{aligned} A^k &= A^{k-1}([B_1, C_1] + \ldots + [B_s, C_s]) \\ &= A^{k-1}(B_1C_1 - C_1B_1 + \ldots + B_sC_s - C_sB_s) \\ &= (B_1A^{k-1}C_1 - A^{k-1}C_1B_1) + \ldots + (B_sA^{k-1}C_s - A^{k-1}C_sB_s) \\ &= [B_1, A^{k-1}C_1] + \ldots + [B_s, A^{k-1}C_s], \end{aligned}$$

and therefore $\operatorname{Tr} A^k = 0$ (see Properties 1° and 2° of a trace). Hence the operator A is nilpotent. □

It follows from this criterion that *for any linear Lie algebra $\mathfrak{g}$ the intersection $\mathfrak{z} \cap \mathfrak{g}^2$ of its centre and the ideal $\mathfrak{g}^2$ consists of nilpotent operators.* Indeed, any operator A in $\mathfrak{g}^2$ is of the form (1), where $B_1, C_1, \ldots, B_s, C_s \in \mathfrak{g}$, and if $A \in \mathfrak{z}$ then $[A, B_1] = 0, \ldots, [A, B_s] = 0$. □

In a similar fashion one can prove that *for every Abelian ideal $\mathfrak{a}$ of a linear Lie algebra $\mathfrak{g}$ the ideal $[\mathfrak{a}, \mathfrak{g}]$ consists of nilpotent operators.*

More exact results can be obtained under the assumption that the linear Lie algebra $\mathfrak{g}$ is *irreducible*, i.e. that $\mathscr{V}$ has no nontrivial subspaces invariant under all operators in $\mathfrak{g}$.

For any subset $\mathfrak{a}$ of a linear Lie algebra $\mathfrak{g}$ acting in a space $\mathscr{V}$ the symbol $\mathfrak{a}\mathscr{V}$ will denote the span of all vectors of the form Ax, where $A \in \mathfrak{a}$ and $x \in \mathscr{V}$.

It is easy to see that *if $\mathfrak{a}$ is an ideal, then the subspace $\mathfrak{a}\mathscr{V}$ is invariant under all operators in $\mathfrak{g}$.* Indeed, if $A \in \mathfrak{a}$, $B \in \mathfrak{g}$ and $x \in \mathscr{V}$, then

$$B(Ax) = [B, A]x + A(Bx) \in \mathfrak{a}\mathscr{V},$$

since $[B, A] \in \mathfrak{a}$. □

It follows that *if a linear Lie algebra $\mathfrak{g}$ is irreducible, then there is a nonnilpotent operator in every nonzero ideal $\mathfrak{a}$ of it.* Indeed, if all operators in $\mathfrak{a}$ are nilpotent, i.e. if $\mathfrak{a}$ is a nilalgebra, then by Proposition 3 the ideal $\mathfrak{a}$ is associatively nilpotent. Let m be the smallest number with the property that the product of any m elements in $\mathfrak{a}$ is zero. Then in the

series of subspaces

$$\mathscr{P}_1 = \mathfrak{a}\mathscr{V},\ \mathscr{P}_2 = \mathfrak{a}\mathscr{P}_1,\ \ldots,\ \mathscr{P}_{m-1} = \mathfrak{a}\mathscr{P}_{m-2},\ \mathscr{P}_m = \mathfrak{a}\mathscr{P}_{m-1}$$

the subspace $\mathscr{P}_m$ is zero and $\mathscr{P}_{m-1} \neq 0$. According to the preceding statement (which was applied $m - 1$ times) $\mathscr{P}_{m-1}$ is invariant under every operator in $\mathfrak{g}$. Hence by irreducibility $\mathscr{P}_{m-1} = \mathscr{V}$ and therefore $\mathscr{P} = \mathfrak{a}\mathscr{V} = \mathfrak{a}\mathscr{P}_{m-1} = \mathscr{P}_m = 0$, which is possible only when $\mathfrak{a} = 0$. □

Applying this general statement to the ideal $\mathfrak{z} \cap \mathfrak{g}^2$ we immediately see that *for any linear irreducible Lie algebra* $\mathfrak{g}$ *we have*

$$\mathfrak{z} \cap \mathfrak{g}^2 = 0.$$

Besides, we see that *any Abelian ideal* $\mathfrak{a}$ *of a linear irreducible Lie algebra* $\mathfrak{g}$ *is in its centre* $\mathfrak{z}$. Indeed, since there are no nonnilpotent operators in the ideal $[\mathfrak{a}, \mathfrak{g}]$ this ideal is zero, but the equation $[\mathfrak{a}, \mathfrak{g}] = 0$ implies exactly that $\mathfrak{a} \subset \mathfrak{z}$. □

Definition 5. A Lie algebra $\mathfrak{g}$ is said to be *reductive* if every Abelian ideal of it is in its centre $\mathfrak{z}$ and $\mathfrak{z} \cap \mathfrak{g}^2 = 0$.

We have thus proved that *any linear irreducible algebra is reductive.*

Let $\mathfrak{g}$ be a reductive Lie algebra. Since $\mathfrak{z} \cap \mathfrak{g}^2 = 0$, we can extend $\mathfrak{g}^2$ to a subspace $\mathfrak{m}$ such that $\mathfrak{g} = \mathfrak{z} \oplus \mathfrak{m}$, and since $[\mathfrak{g}, \mathfrak{m}] \subset [\mathfrak{g}, \mathfrak{g}] \subset \mathfrak{m}$, the subspace $\mathfrak{m}$ is an ideal. Moreover, it is easy to see that every ideal $\mathfrak{a}$ in $\mathfrak{m}$ is an ideal in $\mathfrak{g}$ as well (since $\mathfrak{g} = \mathfrak{z} + \mathfrak{m}$, we have $[\mathfrak{g}, \mathfrak{a}] \subset [\mathfrak{g}, \mathfrak{a}] + [\mathfrak{m}, \mathfrak{a}] = [\mathfrak{m}, \mathfrak{a}] \subset \mathfrak{a}$). Therefore if the ideal $\mathfrak{a} \subset \mathfrak{m}$ is Abelian, then $\mathfrak{a} \subset \mathfrak{z}$ and hence $\mathfrak{a} = 0$. Thus the ideal $\mathfrak{m}$ has no nonzero Abelian ideals and is therefore semisimple.

Conversely, if a Lie algebra $\mathfrak{g}$ is of the form $\mathfrak{z} \oplus \mathfrak{m}$, where $\mathfrak{m}$ is a semisimple ideal, then $\mathfrak{g}^2 = \mathfrak{m}^2 \subset \mathfrak{m}$ and so $\mathfrak{z} \cap \mathfrak{g}^2 = 0$. Besides, under the natural epimorphism $\mathfrak{g} \to \mathfrak{g}/\mathfrak{z}$ every Abelian ideal $\mathfrak{a}$ of $\mathfrak{g}$ can be mapped into an Abelian ideal of the semisimple algebra $\mathfrak{g}/\mathfrak{z} \approx \mathfrak{m}$, i.e. into zero. Therefore $\mathfrak{a} \subset \mathfrak{z}$ and hence the Lie algebra $\mathfrak{g}$ is reductive.

This proves that *a Lie algebra* $\mathfrak{g}$ *is reductive if and only if it is a direct sum of its centre and some semisimple ideal* $\mathfrak{m}$:

$$\mathfrak{g} = \mathfrak{z} \oplus \mathfrak{m}.$$

(Note that in fact $\mathfrak{m} = \mathfrak{g}^2$. Indeed it follows from $\mathfrak{g} = \mathfrak{z} \oplus \mathfrak{m}$ that $\mathfrak{g}^2 = \mathfrak{m}^2$ and, as we show in the next lecture, for any semisimple Lie algebra $\mathfrak{m}$ we have $\mathfrak{m}^2 = \mathfrak{m}$.)

Now it is easy to see that the *radical* $\mathfrak{r}$ *of a reductive Lie algebra* $\mathfrak{g}$ *coincides with its centre* $\mathfrak{z}$. Indeed, under the natural epimorphism $\mathfrak{g} \to \mathfrak{g}/\mathfrak{z}$ the radical $\mathfrak{r}$ is mapped into zero (for the algebra $\mathfrak{g}/\mathfrak{z}$ is isomorphic to the ideal $\mathfrak{m}$ and hence semisimple). Therefore $\mathfrak{r} \subset \mathfrak{z}$ and hence $\mathfrak{r} = \mathfrak{z}$. □

So a *reductive Lie algebra is solvable if and only if it is Abelian.*

Thus, in particular, *every linear irreducible solvable Lie algebra is Abelian.*

To apply this statement to not only irreducible algebras we first prove one general lemma from linear algebra which relates to a linear operator A, in a linear vector space $\mathscr{V}$ having an invariant subspace $\mathscr{P}$. As we know, such an operator induces an operator $A_1: \mathscr{P} \to \mathscr{P}$ on $\mathscr{P}$ and an operator A_2: $\mathscr{V}/\mathscr{P} \to \mathscr{V}/\mathscr{P}$ on $\mathscr{V}/\mathscr{P}$.

Lemma 1. *If operators A_1 and A_2 are nilpotent, then the operator A is also nilpotent.*

Proof. Let $A_1^{k_1} = 0$ and $A_2^{k_2} = 0$. Then A^{k_2} sends $\mathscr{V}$ to $\mathscr{P}$ while A^{k_1} sends $\mathscr{P}$ to zero. Therefore $A^{k_1+k_2} = A^{k_1}A^{k_2}$ sends $\mathscr{V}$ to 0, i.e. $A^{k_1+k_2} = 0$. □

Now it is easy to see that *if $\mathfrak{g}$ is a linear solvable Lie algebra and the operator $A \in \mathfrak{g}$ is nilpotent, then for any operator $B \in \mathfrak{g}$ the operator AB is also nilpotent.* Indeed, proceed by induction on the dimension n of a vector space $\mathscr{V}$ in which a Lie algebra $\mathfrak{g}$ acts, considering that given $n = 1$ the statement is trivial. If $\mathscr{V}$ has no nontrivial subspaces invariant under every operator in $\mathfrak{g}$, i.e. if $\mathfrak{g}$ is irreducible, then according to the foregoing $\mathfrak{g}$ is Abelian and hence $AB = BA$. Therefore $(AB)^k = A^kB^k$ for any $k \geqslant 0$ and hence $(AB)^k = 0$ when $A^k = 0$. If there is a nontrivial invariant subspace $\mathscr{P}$ in $\mathscr{V}$, then restricting all operators in $\mathfrak{g}$ to $\mathscr{P}$ we obtain in $\mathscr{P}$ an algebra of operators which is a homomorphic image of the algebra $\mathfrak{g}$ and is therefore solvable. Hence, by induction hypothesis, the operator AB on $\mathscr{P}$ is nilpotent. Similarly, going over to the factor space $\mathscr{V}/\mathscr{P}$ we see that the operator AB induces there a nilpotent operator. By Lemma 1 therefore AB is a nilpotent operator. □

Note that in general $AB \notin \mathfrak{g}$.

Similarly it can be proved that *for any linear Lie algebra* $\mathfrak{g}$ *with radical* $\mathfrak{r}$ *the ideal* $[\mathfrak{g}, \mathfrak{r}]$ *consists of nilpotent operators.* Indeed, if $\mathfrak{g}$ is irreducible, then, as we know, $\mathfrak{r} = \mathfrak{z}$ and therefore $[\mathfrak{g}, \mathfrak{r}] = 0$. Hence in this case the statement is automatically true. In the general case we again proceed by induction on $\dim \mathscr{V}$. Let $\mathscr{P}$ be a subspace in $\mathscr{V}$ invariant under all operators in $\mathfrak{g}$. Then, restricting all operators in $\mathfrak{g}$ to $\mathscr{P}$ we obtain in $\mathscr{P}$ an operator algebra $\mathfrak{g}$ isomorphic to the quotient algebra of $\mathfrak{g}$ mod an ideal (consisting of operators equal to zero on $\mathscr{P}$). By induction hypothesis, the ideal $[\mathfrak{g}', \mathfrak{r}']$, where $\mathfrak{r}'$ is the radical of $\mathfrak{g}'$, consists of nilpotent operators. Since under the epimorphism $\mathfrak{g} \to \mathfrak{g}'$ the ideal $[\mathfrak{g}, \mathfrak{r}]$ is mapped into $[\mathfrak{g}', \mathfrak{r}']$, this proves that any operator A in $[\mathfrak{g}, \mathfrak{r}]$ induces in $\mathscr{P}$ a nilpotent operator. Similarly it can be proved that A induces a nilpotent operator in the factor space $\mathscr{V}/\mathscr{P}$ as well. Hence by Lemma 1 A is a nilpotent operator. □

It follows by the Engel theorem that for any linear Lie algebra $\mathfrak{g}$ the ideal $[\mathfrak{g}, \mathfrak{r}]$ is nilpotent. It is easy to see, however, that this statement is true for arbitrary Lie algebras as well.

Proposition 4. *In any Lie algebra* $\mathfrak{g}$ *the ideal* $[\mathfrak{g}, \mathfrak{r}]$ *is nilpotent.*

Proof. Let $\mathfrak{g}' = \operatorname{ad} \mathfrak{g}$ and let $\mathfrak{r}$ be a radical of the Lie algebra $\mathfrak{g}'$. According to the foregoing, the ideal $[\mathfrak{g}', \mathfrak{r}']$ is nilpotent. On the other hand, under the homomorphism ad: $\mathfrak{g} \to \mathfrak{g}'$ the ideal $[\mathfrak{g}, \mathfrak{r}]$ goes over to $[\mathfrak{g}', \mathfrak{r}']$ and the centre of the algebra $\mathfrak{g}$ serves as the kernel of that homomorphism. Thus factorization of $[\mathfrak{g}, \mathfrak{r}]$ mod an ideal of the centre yields a nilpotent algebra. Hence the ideal $[\mathfrak{g}, \mathfrak{r}]$ is also nilpotent. □

Corollary. *A Lie algebra* $\mathfrak{g}$ *is solvable if and only if the ideal* $\mathfrak{g}^2$ *is nilpotent.*

Proof. If the algebra $\mathfrak{g}$ is solvable, i.e. if $\mathfrak{g} = \mathfrak{r}$, then the ideal $\mathfrak{g}^2 = [\mathfrak{g}, \mathfrak{g}] = [\mathfrak{g}, \mathfrak{r}]$ is nilpotent. Conversely, if $\mathfrak{g}^2$ is nilpotent (and hence solvable), then $\mathfrak{g}$ is solvable, since the quotient algebra $\mathfrak{g}/\mathfrak{g}^2$ is Abelian. □

The ideal $[\mathfrak{g}, \mathfrak{r}]$ is usually called the *nilpotent radical* of a Lie algebra $\mathfrak{g}$. It is contained in the nilradical $\mathfrak{n}$, but is in general different from $\mathfrak{n}$.

Lecture 18

Trace functional · Killing's functional · The trace functional of a representation · The Jordan decomposition of a linear operator · The Jordan decomposition of the adjoint operator · The Cartan theorem on linear Lie algebras · Proving Cartan's criterion for the solvability of a Lie algebra · Linear Lie algebras with a non-singular trace functional · Semisimple Lie algebras · Cartan's criterion for semisimplicity · Casimir operators

We continue the study of linear Lie algebras we began in the preceding lecture.

It is immediate from the properties of a trace that the formula

$$t(A, B) = \operatorname{Tr} AB$$

defines on any Lie algebra $\mathfrak{g}$ some bilinear symmetric functional t. We shall refer to that functional as the *trace functional* of the Lie algebra $\mathfrak{g}$.

A bilinear functional s on $\mathfrak{g}$ is said to be *invariant* (there is no need to explain the origin of this term here) if

$$s([x, y], z) = s(x, [y, z])$$

for any elements $x, y, z \in \mathfrak{g}$, i.e. if all linear operators of the form $\operatorname{ad} y$, $y \in \mathfrak{g}$, are skew-symmetric with respect to s.

Since for any operators A, B and C the trace of the operator $[A, B]C = ABC - BAC$ equals the trace of the operator $A[B, C] = ABC - ACB$, *the trace functional of any linear Lie algebra* $\mathfrak{g}$ *is invariant.*

Let $\mathfrak{r}$ be the radical of a linear Lie algebra $\mathfrak{g}$ and let $A, B \in \mathfrak{g}$ and $C \in \mathfrak{r}$. Since $[B, C] \in [\mathfrak{g}, \mathfrak{r}]$ the operator

$[B, C]$ is nilpotent. Since $\mathfrak{r}$ is an ideal, the subspace $\mathfrak{a}$ of $\mathfrak{g}$ generated by $\mathfrak{r}$ and A has the property that $[\mathfrak{a}, \mathfrak{a}] \subset \mathfrak{r}$. Hence $\mathfrak{a}$ is a subalgebra of $\mathfrak{g}$ and is solvable. Since $\mathcal{A} \in \mathfrak{a}$, $[B, C] \in [\mathfrak{g}, \mathfrak{r}] \subset \mathfrak{r} \subset \mathfrak{a}$, and since in addition the Lie algebra $\mathfrak{a}$ is solvable and the operator $[B, C]$ is nilpotent, the operator $A\,[B, C]$ is also nilpotent. Therefore its trace is zero, i.e. $t\,(A, [B, C]) = 0$. By invariance then $t\,([A, B], C) = 0$. This proves that *in any linear Lie algebra* $\mathfrak{g}$ *the ideals* $\mathfrak{g}^2$ *and* $\mathfrak{r}$ *are orthogonal with respect to the trace functional* t.

In conventional but illustrative notation we have

$$t\,(\mathfrak{g}^2, \mathfrak{r}) = 0.$$

In particular, when $\mathfrak{g} = \mathfrak{r}$ it follows that *in linear solvable Lie algebra* $\mathfrak{g}$

$$t\,(\mathfrak{g}^2, \mathfrak{g}) = 0,$$

i.e. with respect to the trace functional the ideal $\mathfrak{g}^2$ is orthogonal to the entire algebra $\mathfrak{g}$.

To obtain similar results for an arbitrary (in general, nonlinear) Lie algebra $\mathfrak{g}$ we proceed to a linear Lie algebra $\mathfrak{g}' = \operatorname{ad} \mathfrak{g}$. The trace functional defined on that linear algebra will be transferred to a Lie algebra $\mathfrak{g}$ by means of a homomorphism ad. That is, we define on $\mathfrak{g}$ a bilinear symmetric functional $t_{\mathfrak{g}}$ by the formula

$$t_{\mathfrak{g}}\,(x, y) = t\,(\operatorname{ad} x, \operatorname{ad} y) = \operatorname{Tr}\,(\operatorname{ad} x \operatorname{ad} y).$$

Definition 1. A functional $t_{\mathfrak{g}}$ is called *Killing's functional* of a Lie algebra $\mathfrak{g}$.

Since ad is a homomorphism of Lie algebras, *Killing's functional is invariant.*

For any effectively given Lie algebra Killing's functional is usually calculated without any difficulty.

Example 1. Find Killing's functional of the Lie algebra $\mathfrak{gl}\,(n)$ of all $n \times n$ matrices. The basis of this algebra is composed of matrix units E_{ij}.

Since $E_{ij}E_{\alpha\beta} = \delta_{j\alpha}E_{i\beta}$, we have

$$(1)\qquad [X, E_{\alpha\beta}] = \sum_{i=1}^{n} (x_{i\alpha}E_{i\beta} - x_{\beta i}E_{\alpha i}), \quad \alpha, \beta = 1, \ldots, n,$$

for any matrix $X=\sum_{i,j=1}^{n} x_{ij}E_{ij}$ in $\mathfrak{gl}(n)$, so that

$$(\mathrm{ad}\, X)\, E_{\alpha\beta}=\sum_{i=1}^{n}(x_{i\alpha}E_{i\beta}-x_{\beta i}E_{\alpha i})$$

in the Lie algebra $\mathfrak{gl}(n)$.

Hence

$$(\mathrm{ad}\, X\circ \mathrm{ad}\, Y)\, E_{\alpha\beta}=\sum_{i,j=1}^{n}(x_{i\alpha}y_{ji}E_{j\beta}+x_{\beta i}y_{ij}E_{\alpha j})-\sum_{i,j=1}^{n}(x_{i\alpha}y_{\beta j}+x_{\beta j}y_{i\alpha})\, E_{ij}$$

and therefore

$$\mathrm{Tr}\,(\mathrm{ad}\, X\circ \mathrm{ad}\, Y)=n\sum_{i,j=1}^{n}(x_{ij}y_{ji}+x_{ji}y_{ij})-2\sum_{i,j=1}^{n}x_{ii}y_{jj}=2n\,\mathrm{Tr}\,(XY)-2\,\mathrm{Tr}\, X\cdot\mathrm{Tr}\, Y.$$

This proves that *Killing's functional of* $\mathfrak{gl}(n)$ *is expressed by the formula*

$$t_{\mathfrak{gl}(n)}(X,\ Y)=2n\ \mathrm{Tr}\ (XY)-2\ \mathrm{Tr}\ X\cdot\mathrm{Tr}\ Y,$$

i.e. by

$$t_{\mathfrak{gl}(n)}(X,\ Y)=2nt\ (X,\ Y)-2t\ (X,\ E)\cdot t\ (Y,\ E).$$

Note that *this functional is singular*, i.e. that $\mathfrak{gl}(n)^{\perp}\neq 0$. Indeed it is clear that for any scalar matrix aE there is an identity $t_{\mathfrak{gl}(n)}(X,\ aE)=0,\ X\in\mathfrak{gl}(n)$, implying that $aE\in\mathfrak{gl}(n)^{\perp}$.

Example 2. In the Lie algebra $\mathfrak{sl}(n)$ of $n\times n$ matrices with a zero trace the basis consists of matrices

$$E_{ij}^{(0)}=\begin{cases} E_{ij} & \text{if}\quad i\neq j,\\ E_{ii}-E_{nn}, & \text{if}\quad i=j,\end{cases}$$

where $i,\ j=1,\ \dots,\ n$ and $(i,\ j)\neq(n,\ n)$. The matrix $X=\sum_{i,j=1}^{n}x_{ij}E_{ij}$ in $\mathfrak{sl}(n)$ is expressed in terms of that

basis by the formula

$$X = \sum_{\substack{i,\, j=1 \\ (i,\, j)\neq(n,\, n)}} x_{ij} E_{ij}^{(0)}.$$

It is immediate from relation (1) that

$$(\operatorname{ad} X)\, E_{\alpha\beta}^{(0)} = \begin{cases} \sum\limits_{i=1}^{n} (x_{i\alpha} E_{i\beta}^{(0)} - x_{\beta i} E_{\alpha i}^{(0)}), & \text{if} \quad \alpha \neq \beta. \\ \sum\limits_{\substack{i=1 \\ i\neq\alpha}}^{n-1} (x_{i\alpha} E_{i\alpha}^{(0)} - x_{\alpha i} E_{\alpha i}^{(0)}) & \\ - \sum\limits_{i=1}^{n-1} (x_{in} E_{in}^{(0)} - x_{ni} E_{ni}^{(0)}), & \text{if} \quad \alpha = \beta. \end{cases}$$

On carrying out the necessary calculation we obtain for Killing's functional of $\mathfrak{sl}(n)$ the formula

$$t_{\mathfrak{sl}(n)}(X, Y) = 2n \operatorname{Tr}(XY) = 2nt(X, Y).$$

Thus for $\mathfrak{sl}(n)$ *Killing's functional* $t_{\mathfrak{sl}(n)}$ *and the trace functional* t *differ only by a factor.*

Now it is easy to see that in contrast to the previous case the *functional* $t_{\mathfrak{sl}(n)}$ *is nonsingular*, i.e. $\mathfrak{sl}(n)^{\perp} = 0$. Indeed, if $\operatorname{Tr}(XY) = 0$ for any matrix $Y \in \mathfrak{sl}(n)$, then in particular $x_{ij} = \operatorname{Tr}(XE_{ij}) = 0$ for $i \neq j$ and $x_{ii} - x_{nn} = \operatorname{Tr}(X(E_{ii} - E_{nn})) = 0$ for any i. Therefore the matrix X is of the form aE and so in view of the condition $\operatorname{Tr} X = 0$ it is zero.

Example 3. In the Lie algebra $\mathfrak{so}(n)$ of skew-symmetric $n \times n$ matrices the basis consists of matrices

$$E_{[i,\, j]} = \frac{E_{ij} - E_{ji}}{2}, \quad i < j.$$

By the same formula (1), for any matrix $X = \sum\limits_{i,\, j=1}^{n} x_{ij} E_{ij}$ in $\mathfrak{so}(n)$ there is a formula

$$(\operatorname{ad} X)\, E_{[\alpha,\, \beta]} = \sum_{i=1}^{n} (x_{i\alpha} E_{[i,\beta]} - x_{\beta i} E_{[\alpha,\, i]}).$$

For the functional $t_{\mathfrak{so}(n)}$ this yields the formula

$$t_{\mathfrak{so}(n)}(XY) = (n-1)\operatorname{Tr}(XY) = (n-1)\,t(X, Y).$$

Therefore *for* $\mathfrak{so}(n)$ *the functionals* $t_{\mathfrak{so}(n)}$ *and* t *also differ only by a factor.*

Since $x_{ij} = \operatorname{Tr}(XE_{[i,j]})$ for any matrix $X = \sum_{i,j=1}^{n} x_{ij}E_{ij}$ in $\mathfrak{so}(n)$, it follows in particular that, as in the previous case, the *functional* $t_{\mathfrak{so}(n)}$ *is nonsingular.*

The construction of the Killing functional allows a very far-reaching generalization.

Definition 2. A *representation* of a Lie algebra $\mathfrak{g}$ in a vector space $\mathscr{V}$ (called the *space of the representation*) is a homomorphism $\rho: \mathfrak{g} \to [\operatorname{End}\mathscr{V}]$ of the algebra $\mathfrak{g}$ into the Lie algebra $[\operatorname{End}\mathscr{V}]$ of linear operators in $\mathscr{V}$.

Note that giving a representation ρ of a Lie algebra $\mathfrak{g}$ defines in the space $\mathscr{V}$ of ρ the structure of a module (see Lecture 5) over the Lie algebra $\mathfrak{g}$ (by the formula $xv = \rho(x)v$, where $x \in \mathfrak{g}$, $v \in \mathscr{V}$) and, conversely, any module over $\mathfrak{g}$ is the space of ρ for which $\rho(x)v = xv$, $x \in \mathfrak{g}$, $v \in \mathscr{V}$. Thus the concept of module over a Lie algebra $\mathfrak{g}$ and that of representation of a Lie algebra $\mathfrak{g}$ are essentially identical. That these concepts duplicating each other should both remain is due exclusively to tradition.

An example of a representation is a homomorphism ad. This representation is termed *adjoint.*

By using the formula

$$t_\rho(x, y) = t(\rho(x), \rho(y)) = \operatorname{Tr}(\rho(x)\rho(y)),$$

any representation ρ defines a symmetric invariant bilinear functional on $\mathfrak{g}$ known as the *trace functional of the representation.*

Thus the Killing functional is nothing than the trace functional of an adjoint representation:

$$t_{\mathfrak{g}} = t_{\mathrm{ad}}.$$

The trace functional of a linear Lie algebra is in this terminology the trace functional of an identity representation:

$$t = t_{\mathrm{id}}.$$

Proposition 1. *In every Lie algebra $\mathfrak{g}$ the ideals $\mathfrak{g}^2$ and $\mathfrak{r}$ are orthogonal with respect to the trace functional of any representation ρ. In particular, these ideals are orthogonal with respect to Killing's functional.*

Proof. Let $x, y \in \mathfrak{g}$ and $z \in \mathfrak{r}$. It is necessary to prove that $t_\rho([x, y], z) = 0$. By definition

$$t_\rho([x, y], z) = t(\rho[x, y], \rho z) = t([\rho x, \rho y], \rho z)$$

and therefore $t_\rho([x, y], z) = 0$ since $[\rho x, \rho y]$ is in the ideal $(\rho\mathfrak{g})^2$ of the linear Lie algebra $\rho\mathfrak{g}$ and ρz is its radical. $\square$

Corollary 1. *In a solvable Lie algebra $\mathfrak{g}$ the ideal $\mathfrak{g}^2$ is orthogonal (with respect to Killing's functional) to the entire algebra:*

$$t_\mathfrak{g}(\mathfrak{g}^2, \mathfrak{g}) = 0. \ \square$$

It turns out that this necessary solvability condition is also a sufficient one:

Proposition 2 (Cartan's criterion for solvability). *A Lie algebra $\mathfrak{g}$ is solvable if and only if $t_\mathfrak{g}(\mathfrak{g}^2, \mathfrak{g}) = 0$.*

The proof of this proposition uses a number of facts from linear algebra. We shall begin by presenting them.

For simplicity we shall assume for the time being the field $\mathbb{K}$ to be algebraically closed (say, to be the field $\mathbb{C}$ of complex numbers).

Let A be a linear operator in a finite-dimensional vector space $\mathscr{V}$. We reduce this operator to Jordan normal form (see II, 16), i.e. we find in $\mathscr{V}$ a basis in which the matrix of the operator A is the direct sum of Jordan cells of the form

$$\begin{Vmatrix} \lambda & 1 & 0 & \dots & 0 \\ 0 & \lambda & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & 0 & \lambda & 1 \\ 0 & \dots & \dots & \dots & \lambda \end{Vmatrix}.$$

By replacing ones by zeros in each of these cells we obtain a diagonalizable operator A_d which has the same characteristic roots and hence the same characteristic polynomial as the operator A. The operator $A_n = A - A_d$ is obviously obtained by replacing all roots λ by zeros. This operator

is nilpotent and commutative with A_d (and hence with A). Moreover, it is easy to see that there is a polynomial $p(T)$ such that $A_d = p(A)$ (any polynomial with the property that $p(\lambda_i) = \lambda_i$ and $p^{(k)}(\lambda_i) = 0$ given $k = 1, \ldots, n_i - 1$ for every characteristic root λ_i of A, where n_i is the multiplicity of the root λ_i) and hence a polynomial $q(T)$ such that $A_n = q(A)$ (it suffices to put $q(T) = T - p(T)$). Therefore any operator commutative with A is commutative with A_d and A_n.

If now $A = A' + A''$, where A' is a diagonalizable operator A'' is a nilpotent operator and the operators A' and A'' are commutative with each other and hence with A, then A' and A'' are commutative with A_d and A_n and we have $A' - A_d = A_n - A''$. But it is easy to see that the difference of two commutative diagonalizable (respectively, nilpotent) operators is a diagonalizable (respectively, nilpotent) operator. Since the only both diagonalizable and nilpotent operator is the zero operator, it follows that the equation $A' - A_d = A_n - A''$ is possible only when $A' = A_d$ and $A'' = A_n$.

This proves the following lemma:

Lemma 1. *Any operator A acting in a finite-dimensional vector space $\mathscr{V}$ can be uniquely represented as the sum*

$$A = A_d + A_n \tag{2}$$

of operators A_d and A_n such that:

(i) *the operator A_d is diagonalizable*;

(ii) *the operator A_n is nilpotent*;

(iii) *the operators A_d and A_n are commutative with each other and with the operator A.*

The operators A_d and A_n are both polynomials in A. □

The operator A_n is called the *nilpotent part* of A and the operator A_d is the *diagonalizable part* of A. (Bourbaki refers to A_d as the *semisimple part* of A). Decomposition (2) is called the *Jordan decomposition* of the operator A.

According to the general definitions, it is possible to associate every linear operator $A: \mathscr{V} \to \mathscr{V}$ with a linear operator ad A acting in the vector space End $\mathscr{V}$ by the formula

$$(\operatorname{ad} A)\,X = AX - XA, \qquad X \in \operatorname{End} \mathscr{V}.$$

Lemma 2. *We have*

$$(\mathrm{ad}\ A)_d = \mathrm{ad}\ A_d, \qquad (\mathrm{ad}\ A)_n = \mathrm{ad}\ A_n.$$

Proof. Let $e_1, \ldots, e_n$ be a basis of a space $\mathscr{V}$ in which the matrix of the operator A_d is diagonal. This means that

$$A_d = \lambda_1 E_{11} + \ldots + \lambda_n E_{nn},$$

where E_{ij} are basis operators defined by the formula

$$E_{ij}e_k = \begin{cases} e_i, & \text{if } k = j \\ 0, & \text{if } k \neq j \end{cases}$$

(these operators constitute the basis of the vector space End $\mathscr{V}$ and their matrices in the basis $e_1, \ldots, e_n$ are the matrix units E_{ij}). Since

$$E_{ij}E_{ab} = \begin{cases} E_{ib}, & \text{if } j = a \\ 0, & \text{if } j \neq a \end{cases}$$

we have

$$(\mathrm{ad}\ A_d)\ E_{ij} = (\lambda_i - \lambda_j)\ E_{ij}.$$

This means that in the basis $\{E_{ij}\}$ the matrix of the operator ad A_d is diagonal (with elements $\lambda_i - \lambda_j$ along the principal diagonal). Thus the operator ad A_d is diagonalizable.

It is clear, on the other hand, that for any $k \geqslant 0$ and any $X \in$ End $\mathscr{V}$ the operator $(\mathrm{ad}\ A_n)^k\ X$ is the sum of operators $\pm A_n^i X A_n^j$, where $i + j = k$. Therefore if $A_n^m = 0$, then $(\mathrm{ad}\ A_n)^{2m-1} = 0$, i.e. the operator ad A_n is nilpotent.

Finally, since ad is a homomorphism of Lie algebras, we have $[\mathrm{ad}\ A_d,\ \mathrm{ad}\ A_n] = \mathrm{ad}\ [A_d,\ A_n] = 0$ and $\mathrm{ad}\ A_d + \mathrm{ad}\ A_n = \mathrm{ad}\ (A_d + A_n) = \mathrm{ad}\ A$, i.e. the operators ad A_d and ad A_n are commutative and their sum is equal to the operator ad A.

Thus ad A_d and ad A_n have with respect to ad A characteristic properties (i) to (iii) of Lemma 1. Therefore ad A $= (\mathrm{ad}\ A)_d$ and $\mathrm{ad}\ A_n = (\mathrm{ad}\ A)_n$. □

Corollary. *Operators* ad A_d *and* ad A_n *are polynomials in the operator* ad A. □

Now we can prove our key proposition about linear Lie algebras:

Proposition 3 (Cartan's criterion). *If the trace functional of a linear Lie algebra* $\mathfrak{g}$ *is identically zero, then* $\mathfrak{g}$ *is solvable.*

Proof. Let A be an operator in $\mathfrak{g}^2$ and let $\lambda_1, \ldots, \lambda_n$ be all its eigenvalues (characteristic roots) repeated as many times as their multiplicity is. Proposition 3 is immediate from the following lemma:

Lemma. *For any additive mapping* $\beta: \mathbb{K} \to \mathbb{K}$ *of the field* $\mathbb{K}$ *into itself (i.e. such that* $\beta(a+b) = \beta a + \beta b$*)*

$$\beta(\lambda_1)\lambda_1 + \ldots + \beta(\lambda_n)\lambda_n = 0.$$

Indeed, the field $\mathbb{K}$ is a vector space (finite-dimensional) over the field $\mathbb{Q}$ of rational numbers. Choosing a basis $\{u_i, i \in I\}$ of the field $\mathbb{K}$ over $\mathbb{Q}$ (the index set I is infinite but this interferes with nothing) we denote the ith ($i \in I$) coordinate of an element $u \in \mathbb{K}$ in that basis by $\beta_i(u)$. Since $\mathbb{Q} \subset \mathbb{K}$, we may consider $\beta_i: u \mapsto \beta_i(u)$ as an (obviously additive) mapping $\mathbb{K} \to \mathbb{K}$. Hence in the field $\mathbb{K}$, by the lemma,

$$\beta_i(\lambda_1)\lambda_1 + \ldots + \beta_i(\lambda_n)\lambda_n = 0.$$

Passing in this equation to the ith coordinate we get

$$\beta_i(\lambda_1)^2 + \ldots + \beta_i(\lambda_n)^2 = 0,$$

i.e. (since all numbers $\beta_i(\lambda_1), \ldots, \beta_i(\lambda_n)$ are rational)

$$\beta_i(\lambda_1) = 0, \ldots, \beta_i(\lambda_n) = 0.$$

Since the index $i \in I$ is arbitrary, this is possible only when $\lambda_1 = 0, \ldots, \lambda_n = 0$, i.e. when $A_d = 0$. Hence the operator $A = A_n$ is nilpotent.

This proves that the ideal $\mathfrak{g}^2$ is a Lie nilalgebra. Hence, by the Engel theorem, this ideal is nilpotent and so the Lie algebra $\mathfrak{g}$ itself is solvable.

Thus to complete the proof of Proposition 3 it only remains to prove the lemma.

Proof of the lemma. As above, it may be assumed without loss of generality that

$$A_d = \lambda_1 E_{11} + \ldots + \lambda_n E_{nn}.$$

We introduce into consideration an operator

$$D = \beta(\lambda_1) E_{11} + \ldots + \beta(\lambda_n) E_{nn}.$$

If $p(T)$ is a polynomial such that $p(\lambda_i) = \beta(\lambda_i)$ for all i, then $D = p(A_d)$ and therefore $D = p(q(A))$, where $q(T)$ is a polynomial such that $q(A) = A_d$. Consequently D is commutative with A and hence also with A_n (and A_d). But then $(DA_n)^k = D^k A_n^k$ for any $k \geqslant 0$ and therefore the operator DA_n is nilpotent. Hence it has a zero trace:

$$\operatorname{Tr} DA_n = 0$$

and therefore

$$\beta(\lambda_1)\lambda_1 + \ldots + \beta(\lambda_n)\lambda_n = \operatorname{Tr} DA_d = \operatorname{Tr} DA.$$

Thus we only need to prove that $\operatorname{Tr} DA = 0$.

Since $A \in \mathfrak{g}^2$, the algebra $\mathfrak{g}$ has operators $B_1, \ldots, B_s$, $C_1, \ldots, C_s$ such that

$$A = [B_1, C_1] + \ldots + [B_s, C_s],$$

and therefore

$$\begin{aligned}\operatorname{Tr} DA &= \operatorname{Tr} D[B_1, C_1] + \ldots + \operatorname{Tr} D[B_s, C_s] \\ &= \operatorname{Tr}[D, B_1]C_1 + \ldots + \operatorname{Tr}[D, B_s]C_s.\end{aligned}$$

But

$$(\operatorname{ad} D)E_{ij} = (\beta(\lambda_i) - \beta(\lambda_j))E_{ij}$$

and hence $\operatorname{ad} D = g(\operatorname{ad} A_d)$, where $g(T)$ is a polynomial such that $g(\lambda_i - \lambda_j) = \beta(\lambda_i) - \beta(\lambda_j)$ for any i and j. Such a polynomial does exist since at $\lambda_i - \lambda_j = \lambda_a - \lambda_b$

$$\begin{aligned}\beta(\lambda_i) - \beta(\lambda_j) = \beta(\lambda_i - \lambda_j) &= \beta(\lambda_a - \lambda_b) \\ &= \beta(\lambda_a) - \beta(\lambda_b).\end{aligned}$$

Since $\operatorname{ad} A_d$ is, as we know, a polynomial in $\operatorname{ad} A$, this proves that there is a polynomial $f(T)$ such that $\operatorname{ad} D = f(\operatorname{ad} A)$. Since $A, B_i \in \mathfrak{g}$, we have $[A, B_i] \in \mathfrak{g}$, i.e. $(\operatorname{ad} A)B_i \in \mathfrak{g}$. Hence $(\operatorname{ad} A)^m B_i \in \mathfrak{g}$ for any $m \geqslant 0$ and therefore $(\operatorname{ad} D)B_i = f(\operatorname{ad} A)B_i \in \mathfrak{g}$, i.e. $[D, B_i] \in \mathfrak{g}$. So by hypothesis

$$\operatorname{Tr}[D, B_i]C_i = t([D, B_i], C_i) = 0$$

for any $i = 1, \ldots, s$ and therefore $\operatorname{Tr} DA = 0$. $\square$

Note that *Proposition* 3 *is true for Lie algebras over any field* $\mathbb{K}$ *of characteristic* 0 (and not only over an algebraically

closed one). Indeed in passing from the field $\mathbb{K}$ to its algebraic closure $\overline{\mathbb{K}}$ the hypothesis of Proposition 3 remains valid and its conclusion remains true also over $\mathbb{K}$ (a Lie algebra over $\mathbb{K}$ is solvable if it is solvable as the algebra over $\overline{\mathbb{K}}$). □

Corollary 1. *The radical* $\mathfrak{r}$ *of a Lie algebra* $\mathfrak{g}$ *is the annulet of the ideal* $\mathfrak{g}^2$ *with respect to the Killing functional*:

$$\mathfrak{r} = (\mathfrak{g}^2)^{\perp}.$$

Proof. We already know that $t_{\mathfrak{g}}(\mathfrak{g}^2, \mathfrak{r}) = 0$, i.e. $\mathfrak{r} \subset (\mathfrak{g}^2)^{\perp}$. On the other hand, the image $\mathfrak{s}$ of the ideal $(\mathfrak{g}^2)^{\perp}$ in the adjoint algebra ad $\mathfrak{g}$ has obviously the property that on $\mathfrak{s}^2$ the trace functional t is zero. Thus the ideal $\mathfrak{s}^2$ is solvable and hence so is $(\mathfrak{g}^2)^{\perp}$. Consequently $(\mathfrak{g}^2)^{\perp} \subset \mathfrak{r}$. □

Corollary 2. *A Lie algebra is solvable if*

$$t_{\mathfrak{g}}(\mathfrak{g}^2, \mathfrak{g}^2) = 0, \tag{3}$$

i.e. if

$$\operatorname{Tr}(\operatorname{ad} x)^2 = 0 \tag{4}$$

for any element $x \in \mathfrak{g}^2$.

Proof. By the identity

$$\operatorname{Tr}(\operatorname{ad} x + \operatorname{ad} y)^2 = \operatorname{Tr}(\operatorname{ad} x)^2 + 2\operatorname{Tr}(\operatorname{ad} x \operatorname{ad} y) + \operatorname{Tr}(\operatorname{ad} y)^2$$

condition (4) is equivalent to the fact that for any two elements $x, y \in \mathfrak{g}^2$ there is an equation $\operatorname{Tr}(\operatorname{ad} x \operatorname{ad} y) = 0$ implying that the trace functional of the linear Lie algebra ad $\mathfrak{g}^2$ is identically zero. Equivalent to the same fact is, by definition, condition (3). Therefore, if these conditions are satisfied the linear Lie algebra ad $\mathfrak{g}^2$ is solvable. But then so is the algebra $\mathfrak{g}$ since $\mathfrak{g}/\mathfrak{z} \approx \operatorname{ad} \mathfrak{g}$ and the algebra ad $\mathfrak{g}$/ ad $\mathfrak{g}^2$ is Abelian. □

The requirement that $x \in \mathfrak{g}^2$ is essential in this corollary.

Example 4. Consider a three-dimensional Lie algebra with a basis e_1, e_2, e_3, multiplication being defined by the formulas

$$[e_1, e_2] = 0, \quad [e_1, e_3] = ae_1 + be_2, \quad [e_2, e_3] = ce_1 + de_2,$$

where $ad - bc \neq 0$ and $a^2 + d^2 + 2bc \neq 0$. For this Lie algebra the ideal $\mathfrak{g}^2$ is the span of the elements e_1 and e_2

and is therefore an Abelian Lie algebra. Hence the Lie algebra $\mathfrak{g}$ is solvable. Moreover, for any element $x = x_1e_1 + x_2e_2 + x_3e_3$ of $\mathfrak{g}$ the operator ad x has (in the basis e_1, e_2, e_3) a matrix

$$\begin{pmatrix} -ax_3 & -cx_3 & ax_1+cx_2 \\ -bx_3 & -dx_3 & bx_1+dx_2 \\ 0 & 0 & 0 \end{pmatrix}$$

and hence the operator $(\mathrm{ad}\, x)^2$ has a matrix

$$\begin{pmatrix} (a^2+bc)\,x_3^2 & (a+d)\,cx_3^2 & -(a^2+cb)\,x_1x_3-(a+d)\,cx_2\,cx_3 \\ (a+d)\,bx_3^2 & (bc+d^2)\,x_3^2 & -(a+d)\,bx_1x_3-(bc+d^2)\,x_2x_3 \\ 0 & 0 & 0 \end{pmatrix}$$

with a trace $(a^2+d^2+2bc)\,x_3^2$ equal to zero only when $x_3 = 0$ (i.e. when $x \in \mathfrak{g}^2$).

Now we are ready to prove Proposition 2.

Proof of Proposition 2. It suffices to note that if $t_{\mathfrak{g}}(\mathfrak{g}^2, \mathfrak{g}) = 0$, then all the more so $t_{\mathfrak{g}}(\mathfrak{g}^2, \mathfrak{g}^2) = 0$. □

We now consider linear Lie algebras whose trace functional is nonsingular.

Proposition 4. *A linear Lie algebra with a nonsingular trace functional* t *is reductive.*

Proof. Since $t(\mathfrak{g}^2, \mathfrak{r}) = 0$ and t is invariant, we have $t(\mathfrak{g}, [\mathfrak{g}, \mathfrak{r}]) = t(\mathfrak{g}^2, \mathfrak{r}) = 0$, from which in view of nonsingularity we get $[\mathfrak{g}, \mathfrak{r}] = 0$, i.e. $\mathfrak{r} \subset \mathfrak{z}$. Therefore, in particular, any Abelian ideal of $\mathfrak{g}$ is in $\mathfrak{z}$. Further, as was shown in the preceding lecture, any operator A in $\mathfrak{z} \cap \mathfrak{g}^2$ is nilpotent. So is therefore the operator AB for every operator B in $\mathfrak{g}$ (since $AB = BA$) and therefore the trace $\mathrm{Tr}\, AB = t(A, B)$ is zero. In view of the nonsingularity of the functional t this is possible only when $A = 0$. So $\mathfrak{z} \cap \mathfrak{g}^2 = 0$ and hence the Lie algebra $\mathfrak{g}$ is reductive. □

The converse is true only "up to isomorphism". Namely, it can be shown that *any reductive Lie algebra is isomorphic to a linear algebra with a nonsingular trace functional*, but we shall not need this statement and shall not prove it.

Another converse of Proposition 4 is contained in the following proposition which on the contrary is very useful to us:

Proposition 5. *The trace functional of a linear semisimple Lie algebra $\mathfrak{g}$ is nonsingular.*

We first prove two lemmas.

Lemma 3. *Let $\mathfrak{g}$ be a Lie algebra and let t be a symmetric bilinear invariant functional on $\mathfrak{g}$. Then for any ideal $\mathfrak{a}$ of $\mathfrak{g}$ its annulet $\mathfrak{a}^\perp$ with respect to t is also an ideal.*

Proof. If $x \in \mathfrak{a}^\perp$, $y \in \mathfrak{g}$ and $z \in \mathfrak{a}$, then

$$t([x, y], z) = t(x, [y, z]) = 0$$

and therefore $[x, y] \in \mathfrak{a}^\perp$. $\square$

Lemma 4. *Let $\mathfrak{g}$ be a linear semisimple algebra, let $\mathfrak{a}$ be its ideal and $\mathfrak{a}^\perp$ its annulet with respect to the trace functional* t. Then $\mathfrak{a} \cap \mathfrak{a}^\perp = 0$.

Proof. By Lemma 3 the annulet $\mathfrak{a}^\perp$, and hence the intersection $\mathfrak{a} \cap \mathfrak{a}^\perp$, is an ideal, with the trace functional identically zero on the ideal $\mathfrak{a} \cap \mathfrak{a}^\perp$. By Proposition 3 therefore the ideal $\mathfrak{a} \cap \mathfrak{a}^\perp$ is solvable, and hence zero, $\mathfrak{g}$ being semisimple.

Proof of Proposition 5. Applying Lemma 2 to the ideal $\mathfrak{a} = \mathfrak{g}$ we get $\mathfrak{g}^\perp = 0$. This means exactly that the functional t is nonsingular. $\square$

A representation ρ of a Lie algebra $\mathfrak{g}$ is said to be *faithful* if it is a monomorphism, i.e. if it effects an isomorphism of $\mathfrak{g}$ with a linear algebra $\rho(\mathfrak{g})$. Since the trace functional of $\rho(\mathfrak{g})$ is nothing than the trace functional of ρ, Proposition 5 is equivalent to the statement that the *trace functional of any faithful representation of a semisimple Lie algebra is nonsingular.*

In particular, this statement is applicable to the adjoint representation ad (it is faithful, the centre of a semisimple Lie algebra being zero). Since the trace functional of the adjoint representation is exactly Killing's functional, this proves that *Killing's functional of a semisimple Lie algebra $\mathfrak{g}$ is nonsingular.*

For any ideal $\mathfrak{a}$ of $\mathfrak{g}$ therefore its annulet $\mathfrak{a}^\perp$ with respect to Killing's functional $t_\mathfrak{g}$ has an extra dimension, i.e.

$$\dim \mathfrak{a} + \dim \mathfrak{a}^\perp = \dim \mathfrak{g}.$$

On the other hand, since ad effects an isomorphism of $\mathfrak{a}$ with a linear algebra ad $\mathfrak{g}$ which sends $t_\mathfrak{g}$ to the trace functional t of ad $\mathfrak{g}$, by Lemma 4 $\mathfrak{a} \cap \mathfrak{a}^\perp = 0$.

Hence $\mathfrak{g} = \mathfrak{a} \oplus \mathfrak{a}^{\perp}$.

We formulate this statement as a Proposition 6:

Proposition 6. *In a semisimple Lie algebra $\mathfrak{g}$ any ideal $\mathfrak{a}$ is a direct summand, i.e. there is an ideal $\mathfrak{a}^{\perp}$ such that*

$$\mathfrak{g} = \mathfrak{a} \oplus \mathfrak{a}^{\perp}.$$

The additional ideal $\mathfrak{a}^{\perp}$ is the annulet of $\mathfrak{a}$ with respect to Killing's functional.

Corollary. *Any ideal and any quotient algebra of a semisimple Lie algebra $\mathfrak{g}$ are semisimple Lie algebras.*

Proof. If the annulet of a subspace with respect to a nonsingular bilinear functional is a direct complement of that subspace, then the restriction of the functional to the subspace is obviously nonsingular too. On every ideal $\mathfrak{a}$ of $\mathfrak{g}$ therefore Killing's functional is nonsingular. This means that under the isomorphism ad: $\mathfrak{g} \to \text{ad } \mathfrak{g}$ the ideal $\mathfrak{a}$ goes over into a linear Lie algebra ad $\mathfrak{a}$ with a nonsingular trace functional. By Proposition 4, therefore, the algebra ad $\mathfrak{a}$, and hence the ideal $\mathfrak{a}$, is a reductive Lie algebra, i.e. can be decomposed into a direct sum of its centre $\mathfrak{z}$ and a semisimple ideal $\mathfrak{m}$. Since the direct summand of the ideal is obviously the ideal of the entire algebra, the centre $\mathfrak{z}$, the algebra $\mathfrak{g}$ being semisimple, must be zero. Hence the ideal $\mathfrak{a} = \mathfrak{m}$ is semisimple.

The statement about quotient algebras reduces to the statement about ideals since a quotient algebra mod an ideal $\mathfrak{a}$ is isomorphic to an additional ideal a $\mathfrak{a}^{\perp}$. □

It also follows from the nonsingularity of Killing's functional that *for any semisimple Lie algebra $\mathfrak{g}$ we have $\mathfrak{g} = \mathfrak{g}^2$.* Indeed, by Corollary 1 to Proposition 3 the annulet $(\mathfrak{g}^2)^{\perp}$ of the ideal $\mathfrak{g}^2$ with respect to Killing's functional is zero for a semisimple Lie algebra. In view of the nonsingularity of Killing's functional therefore $\mathfrak{g}^2 = \mathfrak{g}$. □

The condition that the Killing functional should be nonsingular is not only necessary but also sufficient for a Lie algebra to be semisimple. To show this we note in the first place that *if the trace functional t_ρ of a representation ρ of a Lie algebra $\mathfrak{g}$ is nonsingular, then ρ is a faithful representation.* Indeed, if $\rho a = 0$, then $t_\rho(a, x) = \text{Tr}(\rho a, \rho x) = 0$ for all $x \in \mathfrak{g}$ and hence $a = 0$. □

In particular, if the Lie algebra $\mathfrak{g}$ has nonsingular Killing's functional, then its adjoint representation is faithful, so that the linear algebra ad $\mathfrak{g}$ is isomorphic to $\mathfrak{g}$ (and the centre of $\mathfrak{g}$ is trivial). Since under this isomorphism the trace functional of ad $\mathfrak{g}$ corresponds to Killing's functional of $\mathfrak{g}$, it is also nonsingular. Hence the linear algebra ad $\mathfrak{g}$ is reductive and, its centre being trivial, semisimple. Also semisimple is therefore the algebra $\mathfrak{g} \approx \operatorname{ad} \mathfrak{g}$.

This proves the following proposition:

Proposition 7 (Cartan's criterion for semisimplicity). *A Lie algebra $\mathfrak{g}$ is semisimple if and only if its Killing's functional is nonsingular.* □

By this proposition and the results of Examples 1 to 3 the *Lie algebras $\mathfrak{sl}(n)$ and $\mathfrak{so}(n)$ are semisimple and the Lie algebra $\mathfrak{gl}(n)$ is not.* □

Now let ρ be a nontrivial (i.e. such that $\rho a \neq 0$ at least for one element $a \in \mathfrak{g}$) representation of a semisimple algebra $\mathfrak{g}$ and let $\mathfrak{k}$ be its kernel. Then by Proposition 6 there is an ideal $\mathfrak{h} = \mathfrak{k}^{\perp}$ in $\mathfrak{g}$, such that $\mathfrak{g} = \mathfrak{k} \oplus \mathfrak{h}$. The representation ρ restricted to $\mathfrak{h}$ is faithful, and since $\mathfrak{h}$ is semisimple (see the corollary to Proposition 6), the trace functional t_ρ of ρ on the ideal $\mathfrak{h}$ is nonsingular. Therefore for any basis $e_1, \ldots, e_n$ of $\mathfrak{h}$ (as a vector space over a field $\mathbb{K}$) there is a t_ρ-dual basis $e^1, \ldots, e^n$ having the property that

$$t_\rho(e_i, e^j) = \delta_i^j, \quad i, j = 1, \ldots, n.$$

For any element $x \in \mathfrak{g}$ we put

$$[x, e_i] = \alpha_i^j(x) e_j, \qquad [x, e^j] = \beta_i^j(x) e_j.$$

Thus $(\alpha_i^j(x))$ is the matrix of restricting a linear operator ad x to $\mathfrak{h}$ in $e_1, \ldots, e^n$ and $(\beta_i^j(x))$ is the matrix of the same operator in $e^1, \ldots, e^n$.

Lemma 5. *For any element $x \in \mathfrak{g}$ there are equations*

$$\alpha_i^j(x) + \beta_i^j(x) = 0, \quad i, j = 1, \ldots, n.$$

Proof. These equations are just another form of the invariance (the skew symmetry of the linear operator ad$x$) of the functional t_ρ:

$$\alpha_i^j(x) = t_\rho([x, e_i], e^j) = -t_\rho(e_i, [x, e^j]) = -\beta_i^j(x). \ \square$$

Lemma 6. *The linear operator*

$$C = \rho(e_i)\,\rho(e^i)$$

is independent of the choice of basis $e_1, \ldots, e_n$.

Proof. For any other basis $e_{i'} = c^i_{i'} e_i$ of the vector space $\mathfrak{h}$ the dual basis can be expressed by the formula $e^{j'} = c^{j'}_j e^j$. Therefore

$$\begin{aligned}\rho(e_{i'})\,\rho(e^{i'}) &= \delta^{i'}_{j'}\rho(e_{i'})\,\rho(e^{j'})\\ &= \delta^{i'}_{j} c^{i}_{i'} c^{j'}_{j}\,\rho(e_i)\,\rho(e^j)\\ &= \delta^i_j \rho(e_i)\,\rho(e^j)\\ &= \rho(e_i)\,\rho(e^i). \quad \square\end{aligned}$$

Definition 3. The linear operator C is called the *Casimir operator* of a representation ρ.

For the trivial representation $\rho = 0$ we put by definition $C = 0$.

Proposition 8. *A Casimir operator is commutative with any operator in* $\rho(\mathfrak{g})$:

$$[C, \rho(x)] = 0 \quad \textit{for any} \quad x \in \mathfrak{g}.$$

When $\rho \neq 0$ *the trace* $\operatorname{Tr} C$ *of the Casimir operator is equal to the dimension* n *of the ideal* $\mathfrak{h}$, *so that the operator is nonzero (and what is more, it is nonnilpotent).*

Proof. By definition,

$$\operatorname{Tr} C = \operatorname{Tr}(\rho(e_i)\,\rho(e^i)) = t_\rho(e_i, e^i) = \delta^i_i = n.$$

Since

$$\begin{aligned}\rho(x)\,C &= \rho(x)\,\rho(e_i)\,\rho(e^i)\\ &= [\rho(x), \rho(e_i)]\,\rho(e^i) + \rho(e_i)\,\rho(x)\,\rho(e^i)\\ &= \rho([x, e_i])\,\rho(e^i) + \rho(e_i)\,\rho(x)\,\rho(e^i)\\ &= \alpha^j_i(x)\,\rho(e_j)\,\rho(e^i) + \rho(e_i)\,\rho(x)\,\rho(e^i)\end{aligned}$$

and similarly

$$C\rho(x) = -\beta^j_i(x)\,\rho(e_j)\,\rho(e^i) + \rho(e_i)\,\rho(x)\,\rho(e^i),$$

we have $C\rho(x) - \rho(x)\,C = 0$ by Lemma 2. $\square$

A representation ρ is said to be *irreducible* if so is the linear Lie algebra $\rho(\mathfrak{g})$. Such a representation is nontrivial (when $\dim \mathscr{V} > 0$).

Corollary. *The Casimir operator of an irreducible representation of a semisimple Lie algebra is invertible.*

Proof. Since C is commutative with $\rho(x)$, the kernel of the operator C is invariant under all operators $\rho(x)$ and hence, being irreducible, is zero. $\square$

Lecture 19

Cohomologies of Lie algebras • The Whitehead theorem • The Fitting decomposition • The generalized Whitehead Theorem • The Whitehead lemmas • The Weyl complete reducibility theorem • Extensions of Abelian Lie algebras

We begin this lecture with some general constructions whose genesis and meaning can be explained only within homological algebra and in connection with the topological theory of cohomology groups of Lie groups. We shall do it briefly in the next lecture and for the present be satisfied with a purely formal presentation without any motivations.

Let $\mathfrak{g}$ be a Lie algebra, as ever finite-dimensional and over a field $\mathbb{K}$ of characteristic 0, and let $\mathscr{V}$ be a module over $\mathfrak{g}$ having as a vector space over $\mathbb{K}$ a finite dimension (in other words, a space of some finite-dimensional representation ρ of $\mathfrak{g}$).

Definition 1. A function $u = u(x_1, \ldots, x_m)$ of m independent variables $x_1, \ldots, x_m \in \mathfrak{g}$ which takes on values in the module $\mathscr{V}$ is said to be an *m-dimensional cochain* of the Lie algebra $\mathfrak{g}$ over $\mathscr{V}$ if:

(a) the function is skew-symmetric, i.e. if it changes sign when any pair of independent variables is interchanged;

(b) the function is linear in every independent variable (with the values of the other independent variables fixed).

When $m = 1$ condition (a) is meaningless, so that an arbitrary linear mapping $u: \mathfrak{g} \to \mathscr{V}$ is a cochain, and when $m = 0$ it is assumed in accordance with the general conventions about functions with a zero number of independent variables that u is an element of $\mathscr{V}$.

All m-dimensional cochains constitute in an obvious way a vector space $C^m(\mathfrak{g}; \mathscr{V})$.

We set, for any cochain $u \in C^m(\mathfrak{g}; \mathscr{V})$ and any elements $x_1, \ldots, x_{m+1} \in \mathfrak{g}$:

$$(\delta u)(x_1, \ldots, x_{m+1}) = \sum_{i+1}^{m+1} (-1)^{i+1} x_i u(x_1, \ldots, \hat{x}_i, \ldots, x_{m+1})$$
$$+ \sum_{i+1}^{m} \sum_{j=i+1}^{m+1} (-1)^{i+j} u([x_i, x_j], x_1, \ldots, \hat{x}_i, \ldots, \hat{x}_j, \ldots, x_{m+1}),$$

where the symbol ^ over the independent variable means that the latter must be omitted.

It is clear that the function δu defined by that formula is linear in each independent variable and, as calculation shows, skew-symmetric, i.e. it is an $m+1$-dimensional cochain. The resulting mapping

$$\delta \colon C^m(\mathfrak{g}, \mathscr{V}) \to C^{m+1}(\mathfrak{g}, \mathscr{V})$$

is obviously linear.

When $m = 0$

$$(\delta u)(x) = xu,$$

when $m = 1$

$$(\delta u)(x, y) = xu(y) - yu(x) - u([x, y]),$$

when $m = 2$

$$(\delta u)(x, y, z) = xu(y, z) - yu(x, z) + zu(x, y)$$
$$- u([x, y], z) + u([x, z], y) - u([y, z], x).$$

The basic property of the mapping δ is that if twice repeated it is zero:

$$\delta \circ \delta = 0.$$

For example, when $m = 0$

$$(\delta\delta u)(x, y) = x(yu) - y(xu) - [x, y]u = 0,$$

and when $m = 1$

$$(\delta\delta u)(x, y, z) = x(yu(z) - zu(y) - u([y, z])$$
$$- y(xu(z) - zu(x) - u([x, z]))$$
$$+ z(xu(y) - yu(x) - u([x, y]))$$

$$\begin{aligned}&- [x, y]\, u(z) + zu([x, y]) + u([[x, y], z])\\ &+ [x, z]\, u(y) - yu([x, z]) - u([[x, z], y])\\ &- [y, z]\, u(x) + xu([y, z]) + u([[y, z], x])\\ &= 0.\end{aligned}$$

The calculation in the general case is tedious but quite feasible if certain care is exercised. It will be left to the reader.

Definition 2. A cochain u for which $\delta u = 0$ is called a *cocycle* and a cochain u of the form δv is a *coboundary*.

All cocycles form a subspace $Z^m(\mathfrak{g}; \mathscr{V})$ of the vector space $C^m(\mathfrak{g}; \mathscr{V})$ (the kernel of the mapping $\delta: C^m(\mathfrak{g}; \mathscr{V}) \to C^{m+1}(\mathfrak{g}; \mathscr{V})$) and all coboundaries (for $m > 0$) form a subspace $B^m(\mathfrak{g}; \mathscr{V})$ of $C^m(\mathfrak{g}; \mathscr{V})$ (the image of $\delta: C^{m-1}(\mathfrak{g}; \mathscr{V}) \to C^m(\mathfrak{g}; \mathscr{V})$). The relation $\delta \circ \delta = 0$ means that

$$B^m(\mathfrak{g}; \mathscr{V}) \subset Z^m(\mathfrak{g}; \mathscr{V})$$

for any $m > 0$, so that a factor space

$$H^m(\mathfrak{g}; \mathscr{V}) = Z^m(\mathfrak{g}; \mathscr{V})/B^m(\mathfrak{g}; \mathscr{V})$$

is defined.

When $m = 0$ we agree to assume that $H^0(\mathfrak{g}; \mathscr{V}) = Z^0(\mathfrak{g}; \mathscr{V})$, so that $H^0(\mathfrak{g}; \mathscr{V})$ is nothing than a subspace of the module $\mathscr{V}$ consisting of the *invariant elements* of $\mathscr{V}$, i.e. of elements u such that $xu = 0$ for any $x \in \mathfrak{g}$.

When $m = 1$ cocycles are characterized by the relation

$$u([x, y]) = xu(y) - yu(x), \tag{1}$$

and when $m = 2$ by the relation

$$\begin{aligned}u([x, y], z) + u([y, z], x) + u([z, x], y)\\ = xu(y, z) + yu(z, x) + zu(x, y).\end{aligned} \tag{2}$$

The equation $H^1(\mathfrak{g}; \mathscr{V}) = 0$ means that relation (1) implies the existence of an element $v \in \mathscr{V}$ such that

$$u(x) = xv$$

and the equation $H^2(\mathfrak{g}; \mathscr{V}) = 0$ implies that of a linear mapping $v: \mathfrak{g} \to \mathscr{V}$ such that

$$u(x, y) = xv(y) - yv(x) - v([x, y]).$$

In what follows we in fact need only the last two statements.

Suppose now that $\mathfrak{g}$ is a semisimple Lie algebra. Then a Casimir operator $C = \rho(e_i)\rho(e^i)$ of a representation ρ is defined, with $e_1, \ldots, e_n$ a basis of an ideal $\mathfrak{h}$ supplementary to the kernel of ρ and $e^1, \ldots, e^n$ its dual basis with respect to the trace functional t_ρ.

Proposition 1 (Whitehead theorem). *If the operator C is invertible, then*

$$H^m(\mathfrak{g}; \mathscr{V}) = 0 \quad \textit{for any} \quad m \geqslant 0.$$

Proof. Let $m = 0$. If $xv = 0$ for all $x \in \mathfrak{g}$, then $Cv = 0$ and hence $v = 0$. Thus $H^0(\mathfrak{g}; \mathscr{V}) = 0$.

Let $m > 0$ and let $u \in Z^m(\mathfrak{g}; \mathscr{V})$. Then

$$\sum_{i=1}^{m+1}(-1)^{i+1}x_i u(x_1, \ldots, \hat{x}_i, \ldots, x_{m+1}) + \sum_{i=1}^{m}\sum_{j=i+1}^{m+1}(-1)^{i+j}u([x_i, x_j], x_1, \ldots, \hat{x}_i, \ldots, \hat{x}_j, \ldots, \hat{x}_{m+1}) = 0$$

for any elements $x_1, \ldots, x_m, x_{m+1} \in \mathfrak{g}$. On substituting for x_{m+1} the element e_k of $\mathfrak{h}$, multiplying by e^k and summing over k we obtain an identity

$$\begin{aligned}(3)\quad &\sum_{i=1}^{m}(-1)^{i+1}e^k(x_i u(x_1, \ldots, \hat{x}_i, \ldots, x_m, e_k)) \\ &+ (-1)^{n+2}e^k(e_k u(x_1, \ldots, x_n)) \\ &+ \sum_{i=1}^{m-1}\sum_{j=i+1}^{m}(-1)^{i+j}e^k u([x_i, x_j], x_1, \ldots, \hat{x}_i, \ldots, \hat{x}_j, \ldots, x_m, e_k) \\ &+ \sum_{i=1}^{m}(-1)^{i+m+1}e^k u([x_k, e_k], x_1, \ldots, \hat{x}_i, \ldots, x_m) = 0,\end{aligned}$$

that holds for any $x_1, \ldots, x_m \in \mathfrak{g}$.

Since $xu = \rho(x)u$, the term $(-1)^{n+2}e^k(e_k u(x_1, \ldots, x_m))$ in (3) is nothing than $(-1)^{n+2}Cu(x_1, \ldots, x_m)$ and since

$e(xu) = [e, x]\,u + x\,(eu)$, the first sum in that identity is

$$(4)\qquad \sum_{i=1}^{m} (-1)^{i+1} [e^k, x_i]\, u(x_1, \ldots \hat{x}_i, \ldots, x_m, e_k)$$
$$+\sum_{i=1}^{m} (-1)^{i+1} x_i\,(e^k u(x_1, \ldots, \hat{x}_i, \ldots, x_m, e_k))$$
$$= \sum_{i=1}^{m} (-1)^{i} \beta_l^k (x_i)\, e^l u(x_1, \ldots, \hat{x}_i, \ldots, \hat{x}_m, e_k)$$
$$+ \sum_{i=1}^{m} (-1)^{i+1} x_i v(x_1, \ldots, \hat{x}_i, \ldots, x_m),$$

where, just as in Lemma 2 of the preceding lecture,

$$\beta_l^k(x) = t_\rho([x, e^k], e_l),$$

and

$$v(y_1, \ldots, y_{m-1}) = e^k u(y_1, \ldots, y_{m-1}, e_k)$$

for any $y_1, \ldots, y_{m-1} \in \mathfrak{g}$.

But the last sum in (3) is

$$\sum_{i=1} (-1)^{i+m+1} \alpha_k^l (x_i)\, e^k u(e_l, x_1, \ldots, \hat{x}_i, \ldots, x_m)$$
$$= \sum_{i=1}^{m} (-1)^{i} \alpha_l^k (x_i)\, e^l u(x_1, \ldots, \hat{x}_i, \ldots, x_m, e_k),$$

where $\alpha_k^l(x) = t_\rho([x, e_k], e^l)$. Therefore, by Lemma 2 of the preceding lecture, the last sum in (3) and the first sum in (4) cancel out.

Since the double sum in (3) can be written as

$$\sum_{i=1}^{m-1} \sum_{j=i+1}^{m} (-1)^{i+j} v([x_i, x_j], x_1, \ldots, \hat{x}_i, \ldots, \hat{x}_j, \ldots, x_m),$$

this proves that

$$(-1)^{n+2} Cu(x_1, \ldots, x_m) + \sum_{i=1}^{m} (-1)^{i+1} x_i v(x_1, \ldots, \hat{x}_i, \ldots, x_m)$$
$$+ \sum_{i=1}^{m-1} \sum_{j=i+1}^{m} (-1)^{i+j} v([x_i, x_j], x_1, \ldots, \hat{x}_i, \ldots, \hat{x}_j,$$
$$\ldots, x_m) = 0,$$

i.e. that

$$(-1)^{n+2}\, Cu\,(x_1, \ldots, x_m) + (\delta v)\,(x_1, \ldots, x_m) = 0.$$

It follows that on putting

$$w\,(x_1, \ldots, x_m) = (-1)^{n+1}\, C^{-1} v\,(x_1, \ldots, x_m)$$

we obtain a cochain $w \in C^{m-1}(\mathfrak{g}; \mathscr{V})$ such that $u = \delta w$.

Thus every m-dimensional cocycle of the algebra $\mathfrak{g}$ over $\mathscr{V}$ is a coboundary and so $H^m(\mathfrak{g}; \mathscr{V}) = 0$. □

Recall that a linear operator C acting in a vector space $\mathscr{V}$ is said to be a direct sum $A \oplus B$ of an operator A acting in a subspace $\mathscr{P} \subset \mathscr{V}$ and an operator B acting in a subspace $\mathscr{Q} \subset \mathscr{V}$ if, first, $\mathscr{V} = \mathscr{P} \oplus \mathscr{Q}$, second, the subspaces $\mathscr{P}$ and $\mathscr{Q}$ are invariant under C and, third, the operators induced in $\mathscr{P}$ and $\mathscr{Q}$ by C coincide, respectively, with A and B. In conventional but illustrative form

$$A \oplus B = \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}$$

(cf. II, 14).

We use the following lemma to investigate vector spaces $H^m(\mathfrak{g}; \mathscr{V})$ in the case, where the Casimir operator C is irreversible:

Lemma 1. *Any linear operator C in a finite-dimensional vector space $\mathscr{V}$ can be uniquely decomposed into a direct sum*

$$C = A \oplus B \tag{5}$$

of an invertible operator A and a nilpotent operator B.

Proof. Since $\mathscr{V}$ is finite-dimensional, the descending chain of subspaces

$$\mathscr{V} \supset \operatorname{Im} C \supset \operatorname{Im} C^2 \supset \ldots \supset \operatorname{Im} C^k \supset \ldots \tag{6}$$

stabilizes, i.e. there is k such that $\operatorname{Im} C^k = \operatorname{Im} C^{k+1}$. We put $\mathscr{P} = \operatorname{Im} C^k$. Clearly, $\mathscr{P}$ is invariant under C and the induced operator $A\colon \mathscr{P} \to \mathscr{P}$ (being a subjective operator) is invertible.

For the same reasons there stabilizes the ascending chain of subspaces

$$0 \subset \operatorname{Ker} C \subset \operatorname{Ker} C^2 \subset \ldots \subset \operatorname{Ker} C^l \subset \ldots, \tag{7}$$

i.e. there is l such that $\operatorname{Ker} C^l = \operatorname{Ker} C^{l+1}$. The subspace $\mathcal{Q} = \operatorname{Ker} C^l$ is invariant under C and the induced operator $B\colon \mathcal{Q} \to \mathcal{Q}$ is nilpotent (since $B^l = 0$). On replacing, if necessary, exponent k or l by the largest of them we may assume that $k = l$.

Thus to prove the existence of decomposition (5) it only remains to prove that $\mathcal{V} = \mathcal{P} \oplus \mathcal{Q}$. By hypothesis, for any vector $v \in \mathcal{V}$ there is a vector v_1 such that $C^k v = C^{2k} v_1$ and the vector $v - C^k v$ is in $\mathcal{Q}$. Since $C^k v_1 \in \mathcal{P}$, this proves that $\mathcal{V} = \mathcal{P} \oplus \mathcal{Q}$. If, however, $v \in \mathcal{P} \cap \mathcal{Q}$, i.e. $v = C^k w$ and $C^k v = 0$, then $C^{2k} w = 0$ and hence $w \in \mathcal{Q}$. Consequently $C^k w = 0$, i.e. $v = 0$.

This completes the proof of the existence of (5).

The uniqueness of (5) is immediate from the fact that for any decomposition (5) the corresponding subspaces $\mathcal{P}$ and $\mathcal{Q}$ are uniquely characterized as subspaces in which chains (6) and (7) stabilize. □

Decomposition (3) is called the *Fitting decomposition* of an operator C.

Now suppose again that $\mathcal{V}$ is the space of a representation ρ of a semisimple Lie algebra $\mathfrak{g}$ and C is its Casimir operator. Then the subspaces $\mathcal{P}$ and $\mathcal{Q}$ are invariant under all operators $\rho(x)$, $x \in \mathfrak{g}$, i.e. they are submodules. Indeed, suppose, for example, $v \in \mathcal{P}$. By hypothesis, there is a vector $w \in \mathcal{V}$ such that $v = C^k w$. Let $\rho(x) w = w_1 + w_2$, where $w_1 \in \mathcal{P}$ and $w_2 \in \mathcal{Q}$. Since $C^k w_2 = 0$, we have

$$\rho(x) v = \rho(x) C^k w = C^k \rho(x) w = C^k w_1 \in \mathcal{P}.$$

Similarly if $v \in \mathcal{Q}$ and $C^k v = 0$, then $C^k \rho(x) v = \rho(x) C^k v = 0$ and hence $\rho(x) v \in \mathcal{Q}$. □

Being modules over $\mathfrak{g}$, the vector spaces $\mathcal{P}$ and $\mathcal{Q}$ are the spaces of some representations σ and τ of $\mathfrak{g}$ (the representation ρ is said *to be decomposed into a direct sum* of representations σ and τ). It is clear that the operators A and B in the Fitting decomposition of the Casimir operator C of a representation ρ are the Casimir operators of σ and τ. By Proposition 1, therefore, for any $m \geqslant 0$,

$$H^m(\mathfrak{g};\ \mathcal{P}) = 0.$$

On the other hand, since the Casimir operator B of τ is nilpotent, the representation is trivial (and $B = 0$). This

means that $\mathcal{Q}$ is a direct sum of one-dimensional invariant subspaces on each of which $\mathfrak{g}$ acts trivially. In other words, the $\mathfrak{g}$-module $\mathcal{Q}$ is a direct sum of modules each of which is isomorphic to the field $\mathbb{K}$ with a trivial action of $\mathfrak{g}$ on it. The number of these summands is referred to as the *multiplicity* of $\mathbb{K}$ in $\mathscr{V}$.

It is clear that if the $\mathfrak{g}$-module $\mathscr{V}$ is a direct sum of $\mathfrak{g}$-modules $\mathscr{V}_1, \ldots, \mathscr{V}_s$, then for any $m \geqslant 0$ the vector space $H^m(\mathfrak{g}; \mathscr{V})$ is a direct sum of vector spaces $H^m(\mathfrak{g}; \mathscr{V}_1), \ldots, H^m(\mathfrak{g}; \mathscr{V}_s)$. Together with the foregoing this proves the following proposition which is a generalization of Proposition 1:

Proposition 2. *For any module $\mathscr{V}$ over a semisimple Lie algebra $\mathfrak{g}$ and every $m \geqslant 0$ the vector space $H^m(\mathfrak{g}; \mathscr{V})$ is a direct sum of k copies of a vector space $H^m(\mathfrak{g}; \mathbb{K})$, where k is the multiplicity of $\mathbb{K}$ in $\mathscr{V}$.* □

Thus, to calculate any vector spaces $H^m(\mathfrak{g}; \mathscr{V})$ it suffices to be able to calculate vector spaces $H^m(\mathfrak{g}; \mathbb{K})$.

It is useful to bear in mind in this connection that for cochains over $\mathbb{K}$ the general formula of a coboundary significantly simplifies to assume the form

$$(\delta u)(x_1, \ldots, x_{m+1}) = \sum_{i=1}^{m} \sum_{j=i+1}^{m+1} (-1)^{i+j} u([x_i, x_j], x_1, \ldots, \hat{x}_i, \ldots, \hat{x}_j, \ldots, x_{m+1}).$$

For example, when $m = 0$

$$(\delta u)(x) = 0,$$

when $m = 1$

$$(\delta u)(x, y) = -u([x, y]),$$

and when $m = 2$

$$(\delta u)(x, y, z) = -u([x, y], z) + u([x, z], y) - u([y, z], x).$$

Therefore $H^0(\mathfrak{g}; \mathbb{K}) = \mathbb{K}$ and $H^1(\mathfrak{g}; \mathbb{K})$ is a space of linear functionals $\mathfrak{g} \to \mathbb{K}$ equal zero on $\mathfrak{g}^2$ (i.e. it is the annulet $\operatorname{Ann} \mathfrak{g}^2$ of the subspace $\mathfrak{g}^2$ in the conjugate space $\mathfrak{g}'$).

It was shown in the preceding lecture that a semisimple Lie algebra $\mathfrak{g}$ coincides with its ideal $\mathfrak{g}^2$. For any semisimple Lie algebra therefore $H^1(\mathfrak{g}; \mathbb{K}) = 0$.

By virtue of Proposition 2 this proves

Corollary 1 (Whitehead's first lemma). *For any module $\mathscr{V}$ over a semisimple Lie algebra $\mathfrak{g}$,*

$$H^1(\mathfrak{g}; \mathscr{V}) = 0. \ \square$$

To obtain a similar result at $m = 2$ we set for any element $x \in \mathfrak{g}$ and any functional $\xi: \mathfrak{g} \to \mathbb{K}$

$$x\xi = -\xi \circ \operatorname{ad} x.$$

An easy check shows that the correspondence $(x, \xi) \mapsto x\xi$ defines in the conjugate vector space $\mathfrak{g}'$, a $\mathfrak{g}$-module structure. It makes sense therefore to consider cochains of $\mathfrak{g}$ over the module $\mathfrak{g}'$.

For every $m \geqslant 1$ we define a mapping

$$\varphi: C^m(\mathfrak{g}; \mathbb{K}) \to C^{m-1}(\mathfrak{g}; \mathfrak{g}'),$$

by setting

$$(\varphi u)(x_1, \ldots, x_{m-1})(x) = u(x_1, \ldots, x_{m-1}, x), \quad x_1, \ldots, x_{m-1}, x \in \mathfrak{g}$$

for any cochain $u \in C^m(\mathfrak{g}; \mathbb{K})$. Since

$$\begin{aligned}[\delta(\varphi u)(x_1, \ldots, x_m)](x) &= \sum_{i=1}^{m} (-1)^{i+1} [x_i((\varphi u)(x_1, \ldots, \hat{x}_i, \ldots, x_m))](x) \\ &\quad + \sum_{i=1}^{m-1} \sum_{j=i+1}^{m} (-1)^{i+j} [(\varphi u)([x_i, x_j], x_1, \ldots, \hat{x}_i, \ldots, \hat{x}_j, \ldots, x_m)](x) \\ &= \sum_{i=1}^{m} (-1)^{i} [(\varphi u)(x_1, \ldots, \hat{x}_i, \ldots, x_m)]([x_i, x]) \\ &\quad + \sum_{i=1}^{m-1} \sum_{j=i+1}^{m} (-1)^{i+j} u([x_i, x_j], x_1, \ldots, \hat{x}_i, \ldots, \hat{x}_j, \ldots, x_m, x)\end{aligned}$$

$$= \sum_{i=1}^{m} (-1)^i u(x_1, \ldots, \hat{x}_i, \ldots, x_m, [x_i, x]) + \sum_{i=1}^{m-1} \sum_{j=i+1}^{m} (-1)^{i+j} u([x_i, x_j], x_1, \ldots, \hat{x}_i, \ldots, \hat{x}_j, \ldots, x_m, x) = (\delta u)(x_1, \ldots, x_m, x)$$
$$= [(\varphi(\delta u))(x_1, \ldots, x_m)](x),$$

for any cochain $u \in C^m(\mathfrak{g}; \mathbb{K})$ and any elements $x, x_1, \ldots, x_m \in \mathfrak{g}$, we have $\delta \circ \varphi = \varphi \circ \delta$ from which it follows, in particular, that for any cocycle u the cochain φu is also a cocycle.

For a semisimple Lie algebra $\mathfrak{g}$, given $m = 2$, it follows from Whitehead's first lemma that for any cocycle $u \in Z^2(\mathfrak{g}; \mathbb{K})$ there is a cochain $\xi \in C^0(\mathfrak{g}; \mathfrak{g}') = \mathfrak{g}'$ such that $\varphi u = \delta\xi$. Then for any elements $x, y \in \mathfrak{g}$

$$\begin{aligned} u(x, y) &= ((\varphi u)(x))(y) = ((\delta\xi)(x))(y) \\ &= (x\xi)(y) = -(\xi \circ \operatorname{ad} x)(y) \\ &= -\xi([x, y]) = (\delta\xi)(x, y), \end{aligned}$$

which implies that $u = \delta\xi$. Hence $H^2(\mathfrak{g}; \mathbb{K}) = 0$.

By virtue of Proposition 2 this proves the following corollary:

Corollary 2 (Whitehead's second lemma). *For any module $\mathscr{V}$ over a semisimple Lie algebra $\mathfrak{g}$,*

$$H^2(\mathfrak{g}; \mathscr{V}) = 0. \quad \square$$

When $m = 3$ there are semisimple Lie algebras for which $H^3(\mathfrak{g}; \mathbb{K}) \neq 0$.

The Whitehead lemmas, although reckoned in the class of lemmas, are nevertheless very important, being a key to two principal theorems of the theory of Lie algebras.

A representation ρ of a Lie algebra $\mathfrak{g}$ is said to be *completely reducible* if it is a direct sum of irreducible representations.

Proposition 3 (Weyl theorem). *Any representation ρ of a semisimple Lie algebra $\mathfrak{g}$ over a field $\mathbb{K}$ is completely reducible.*

Before proving this proposition we consider some simple facts from linear algebra.

Let $\mathscr{V}$ be a vector space and let $\mathscr{P}$ be some subspace of it. Consider a subspace $\mathscr{Q}$ complementary to $\mathscr{P}$, i.e. such that

(8) $$\mathscr{V} = \mathscr{P} \oplus \mathscr{Q}.$$

If $u \in \mathscr{V}$ and $u = v + w$, where $v \in \mathscr{P}$ and $w \in \mathscr{Q}$, then by putting $Pu = v$ we obviously obtain an idempotent linear operator (i.e. such that $P^2 = P$) $P: \mathscr{V} \to \mathscr{V}$ with the property that $\operatorname{Im} P = \mathscr{P}$. Such operators are called *projectors on* $\mathscr{P}$. Hence we see that any decomposition of the form (8) defines some projector on $\mathscr{P}$.

Conversely, let $P: \mathscr{V} \to \mathscr{V}$ be a projector on $\mathscr{P}$ and let $\mathscr{Q} = \operatorname{Ker} P$. For any vector $u \in \mathscr{V}$ the vector Pu is in $\mathscr{P}$ (since $Pu = P(Pu)$) and the vector $u - Pu$ is in $\mathscr{Q}$ (since $P(u - Pu) = Pu - P^2u = 0$). Since $u = Pu + (u - Pu)$ this proves that $\mathscr{V} = \mathscr{P} + \mathscr{Q}$. But if $u \in \mathscr{P} \cap \mathscr{Q}$, then, firstly, $u = Pu$ (since $u \in \mathscr{P} = \operatorname{Im} P$ we have $u = Pv$, where $v \in \mathscr{V}$ and therefore $Pu = P(Pv) = Pv = u$) and, secondly, $Pu = 0$ (since $u \in \mathscr{Q}$), which is possible only when $u = 0$. Hence $\mathscr{V} = \mathscr{P} \oplus \mathscr{Q}$.

This proves the following lemma:

Lemma 2. *Subspaces $\mathscr{Q}$ complementary to a subspace $\mathscr{P}$ are in a natural bijective correspondence to projectors on $\mathscr{P}$, every projector P corresponding to its kernel* $\operatorname{Ker} P$. □

If now $\mathscr{V}$ is a module over a Lie algebra $\mathfrak{g}$, then the *subspaces $\mathscr{P} = \operatorname{Im} P$ and $\mathscr{Q} = \operatorname{Ker} P$ are submodules if and only if the operator P is a homomorphism of modules*, i.e. commutative with all operators $\rho(x)$, $x \in \mathfrak{g}$, where ρ is a representation defined by $\mathscr{V}$. Indeed if P is a homomorphism and $u \in \mathscr{P}$ (and hence $u = Pu$), then $xu = \rho(x)u = \rho(x)Pu = P\rho(x)u \in \mathscr{P}$ for any $x \in \mathfrak{g}$. Similarly, if $u \in \mathscr{Q}$, then $P(xu) = \rho(x)P(u) = 0$ and hence $xu \in \mathscr{Q}$. Conversely, if $\mathscr{P}$ and $\mathscr{Q}$ are submodules, then for any elements $u \in \mathscr{V}$ and $x \in \mathfrak{g}$ we have $xu = x(Pu + (u - Pu)) = xPu + x(u - Pu)$, where $xPu \in \mathscr{P}$ and $x(u - Pu) \in \mathscr{Q}$, which shows that $x(Pu) = P(xu)$. □

Proof of Proposition 3. An obvious inductive reasoning (using the fact that ρ is finite-dimensional) shows that to prove Proposition 3 it suffices to establish that for any submodule $\mathscr{P}$ of a $\mathfrak{g}$-module $\mathscr{V}$ there is a decomposition (6) in which $\mathscr{Q}$ is also a submodule, i.e. to prove that *there is a projector $P: \mathscr{V} \to \mathscr{V}$ onto $\mathscr{P}$ which is a homomorphism of modules.*

To this end we consider the set $\mathscr{W}$ of all linear operators $A: \mathscr{V} \to \mathscr{V}$ for which $\operatorname{Im} A \subset \mathscr{F} \subset \operatorname{Ker} A$ (and hence $A^2 = 0$). A calculation shows that $\mathscr{W}$ is a subspace of the vector space $\operatorname{End} \mathscr{V}$ and what is more a module over $\mathfrak{g}$ with respect to the action

$$xA = [\rho(x), A], \qquad x \in \mathfrak{g}, \qquad A \in \mathscr{W}.$$

If now P_0 is a projector on $\mathscr{F}$, then, as is easily seen, $[\rho(x), P_0] \in \mathscr{W}$ for any $x \in \mathfrak{g}$ and hence the formula

$$u(x) = [\rho(x), P_0], \qquad x \in \mathfrak{g},$$

defines some linear mapping $u: \mathfrak{g} \to \mathscr{W}$, i.e. a cochain in $C^1(\mathfrak{g}, \mathscr{W})$. Since by the Jacobi identity

$$xu(y) - yu(x) - u([x, y]) = [\rho(x), [\rho(y), P_0]] \\ -[\rho(y), [\rho(x), P_0]] - [\rho[x, y], P_0] = 0,$$

that cochain is a cocycle. By Whitehead's first lemma therefore there is an operator $A \in W$ such that $u(x) = xA$ for any $x \in \mathfrak{g}$, i.e. such that $[\rho(x), P_0] = [\rho(x), A]$. For the operator $P = P_0 - A$ the last relation implies that it is commutative with all operators of the form $\rho(x)$, $x \in \mathfrak{g}$, i.e. it is a homomorphism of the module $\mathscr{V}$ into itself. We have $Pv \in \mathscr{V}$ for any $v \in \mathscr{V}$ and $Pv = P_0 v = v$ if $v \in \mathscr{F}$, so that P is a projector into $\mathscr{F}$. □

A similar use of Whitehead's second lemma requires some preparations.

We shall say that a Lie algebra $\mathfrak{h}$ is an *extension* of a Lie algebra $\mathfrak{a}$ by means of a Lie algebra $\mathfrak{g}$ if $\mathfrak{a}$ is an ideal in $\mathfrak{h}$ and the quotient algebra $\mathfrak{h}/\mathfrak{a}$ is isomorphic to $\mathfrak{g}$. The last condition implies that there is an epimorphism of Lie algebras $\alpha: \mathfrak{h} \to \mathfrak{g}$ whose kernel is the ideal $\mathfrak{a}$. We assume that epimorphism to be once and for ever chosen and fixed.

The extension $\mathfrak{h}$ is said to be *trivial* if $\mathfrak{h}$ has a subalgebra which is isomorphically mapped under α onto $\mathfrak{g}$.

Clearly, we can always find a linear mapping

$$\beta: \mathfrak{g} \to \mathfrak{h}$$

such that $\alpha \circ \beta = \mathrm{id}_{\mathfrak{g}}$ (a section of the homomorphism α). Then the Lie algebra $\mathfrak{h}$ as a vector space will be decomposed

into a direct sum of an ideal $\mathfrak{a}$ and a subspace Im β. The extension $\mathfrak{h}$ is trivial if and only if the mapping β can be chosen from among the homomorphisms of Lie algebras.

The deviation of β from a homomorphism of algebras is measured by the function $u = u(x, y)$ defined by the formula

$$u(x, y) = [\beta x, \beta y] - \beta[x, y], \quad x, y \in \mathfrak{g}.$$

Since $\alpha u(x, y) = [\alpha\beta x, \alpha\beta y] - \alpha\beta[x, y] = 0$, the function u may be thought of as taking values in the ideal $\mathfrak{a}$. Clearly, this function is linear in both independent variables and skew-symmetric, i.e. it is a two-dimensional cochain of $\mathfrak{g}$ assuming values in the ideal $\mathfrak{a}$.

However, the last conclusion is rather hasty, since the ideal $\mathfrak{a}$ is not in general a $\mathfrak{g}$-module, which is required of the range of cochains. To overcome this difficulty we assume that $\mathfrak{a}^2 = 0$, i.e. that the *algebra* $\mathfrak{a}$ *is Abelian*. Then the formula

$$xa = [\beta x, a], \qquad x \in \mathfrak{g}, \qquad a \in \mathfrak{a},$$

will correctly (regardless of the choice of section β) define a $\mathfrak{g}$-module structure in $\mathfrak{a}$ and therefore we can call the function u a cochain.

Now it is easily seen that a *cochain* $u \in C^2(\mathfrak{g}; \mathfrak{a})$ *is a cocycle*. Indeed, using twice the Jacobi identity we get

$$\begin{aligned}(\delta u)(x, y, z) &= xu(y, z) - yu(x, z) + zu(x, y)\\ &\quad - u([x, y], z) + u([x, z], y) - u([y, z], x)\\ &= [\beta x, [\beta y, \beta z] - \beta[y, z]] - [\beta y, [\beta x, \beta z]\\ &\quad - \beta[x, z]] + [\beta z, [\beta x, \beta y] - \beta[x, y]]\\ &\quad - [\beta[x, y], \beta z] + \beta[[x, y], z] + [\beta[x, z], \beta y]\\ &\quad - \beta[[x, z], y] - [\beta[y, z], \beta x] + \beta[[y, z], x]\\ &= [\beta x, [\beta y, \beta z]] - [\beta y, [\beta x, \beta z]] + [\beta z, [\beta x, \beta y]]\\ &\qquad + \beta([[x, y], z] - [[x, z], y] + [[y, z], x]) = 0\end{aligned}$$

for any elements $x, y, z \in \mathfrak{g}$. □

Let β' be another section of an epimorphism α. Then the difference $v = \beta - \beta'$ may be thought of as a linear mapping

$\mathfrak{g} \to \mathfrak{a}$, i.e. as a cochain in $C^1(\mathfrak{g}; \mathfrak{a})$. Since

$$\begin{aligned}(\delta v)(x, y) &= xv(y) - yv(x) - v([x, y]) \\ &= [\beta x, \beta y - \beta' y] - [\beta' y, \beta x - \beta' x] - \beta[x, y] \\ &+ \beta'[x, y] = ([\beta x, \beta y] - \beta[x, y]) \\ &- ([\beta' x, \beta' y] - \beta'[x, y]),\end{aligned}$$

replacing β by β' involves repacing u by $u - \delta v$. Hence if $u = \delta v$, then the mapping $\beta = \beta - v$ will be a homomorphism of Lie algebras, i.e. the extension $\mathfrak{h}$ will be trivial.

But according to Whitehead's second lemma the condition $u = \delta v$ certainly holds if the Lie algebra is semisimple. This proves the following proposition.

Proposition 4. *Any extension $\mathfrak{h}$ of an Abelian Lie algebra $\mathfrak{a}$ by means of a semisimple Lie algebra $\mathfrak{g}$ is trivial.*

Corollary. *A Lie algebra $\mathfrak{g}$ is reductive if and only if its centre $\mathfrak{z}$ coincides with its radical $\mathfrak{r}$:*

$$\mathfrak{z} = \mathfrak{r}.$$

Proof. We have already proved in Lecture 12 that $\mathfrak{r} = \mathfrak{z}$ for a reductive algebra. Conversely, let $\mathfrak{r} = \mathfrak{z}$. Then $\mathfrak{g}$ is an extension of the Abelian algebra $\mathfrak{z}$ by means of a semisimple algebra $\mathfrak{g}/\mathfrak{r}$. Hence by Proposition 4 we have $\mathfrak{g} = \mathfrak{z} \oplus \mathfrak{m}$, where $\mathfrak{m}$ is a semisimple subalgebra. Since $[\mathfrak{z}, \mathfrak{m}] = 0 \subset \mathfrak{m}$, the semisimple subalgebra $\mathfrak{m}$ is an ideal. Hence $\mathfrak{g}$ is a reductive Lie algebra. $\square$

Lecture 20

The Levi theorem • Simple Lie algebras and simple Lie groups • Cain and unimodular groups • Schur's lemma • The centre of a simple matrix Lie group • An example of a nonmatrix Lie group • De Rham cohomologies • Cohomologies of the Lie algebras of vector fields • Comparison between the cohomologies of a Lie group and its Lie algebra

Every Lie algebra $\mathfrak{g}$ is an extension of its radical $\mathfrak{r}$ by means of the algebra $\mathfrak{g}/\mathfrak{r}$. We say that a Lie algebra $\mathfrak{g}$ *admits a Levi decomposition* if that extension is trivial, i.e. if there is a (clearly semisimple) subalgebra $\mathfrak{m}$ in $\mathfrak{g}$, such that

$$\mathfrak{g} = \mathfrak{r} \oplus \mathfrak{m}.$$

If $\mathfrak{g}$ is semisimple and solvable, it certainly admits a Levi decomposition. By Proposition 4 of the preceding lecture an algebra $\mathfrak{g}$ whose radical $\mathfrak{r}$ is Abelian admits a Levi decomposition.

Proposition 1 (Levi theorem). *Any Lie algebra $\mathfrak{g}$ over a field $\mathbb{K}$ admits a Levi decomposition.*

Proof. We proceed by induction on the dimension $n = \dim \mathfrak{r}$ of the radical of $\mathfrak{g}$. If $n = 0$ or $n = 1$ or if the ideal $\mathfrak{a} = \mathfrak{r}^2$ is zero, then according to the foregoing $\mathfrak{g}$ admits a Levi decomposition. Let $n > 1$ and let $\mathfrak{a} \neq 0$. Then $\dim \mathfrak{r}/\mathfrak{a} < n$, and since $\mathfrak{r}/\mathfrak{a}$ is the radical of the quotient algebra $\mathfrak{g}/\mathfrak{a}$, the algebra $\mathfrak{g}/\mathfrak{a}$ admits a Levi decomposition by induction hypothesis. For $\mathfrak{g}$ this implies that there is a subalgebra $\mathfrak{b}$ in it, such that $\mathfrak{g} = \mathfrak{r} + \mathfrak{b}$ and $\mathfrak{r} \cap \mathfrak{b} = \mathfrak{a}$. The ideal $\mathfrak{a}$ is a solvable ideal of the algebra $\mathfrak{b}$ the quotient algebra $\mathfrak{b}/\mathfrak{a}$ mod which is semisimple (for it is

isomorphic to the semisimple algebra $\mathfrak{g}/\mathfrak{r}$). This means that $\mathfrak{a}$ is the radical of $\mathfrak{b}$, and since $\dim \mathfrak{a} < n$, by induction hypothesis there is a semisimple subalgebra $\mathfrak{m}$ in $\mathfrak{b}$, such that $\mathfrak{b} = \mathfrak{a} \oplus \mathfrak{m}$. But then $\mathfrak{r} \cap \mathfrak{m} = \mathfrak{r} \cap \mathfrak{b} \cap \mathfrak{m} = \mathfrak{a} \cap \mathfrak{m} = 0$ and $\mathfrak{r} + \mathfrak{m} = \mathfrak{r} + \mathfrak{r} \cap \mathfrak{b} + \mathfrak{m} = \mathfrak{r} + \mathfrak{a} + \mathfrak{m} = \mathfrak{r} + \mathfrak{b} = \mathfrak{g}$, so that $\mathfrak{g} = \mathfrak{r} \oplus \mathfrak{m}$. □

We could now proceed directly to the proof of the Ado theorem, but we choose instead to deviate somewhat from our course and consider the validity of the analogue of this theorem for Lie groups. We shall also discuss the interrelations between the formal-algebraic theory of cohomologies of Lecture 19 and cohomology theories known in topology.

In general-algebraic terms a Lie algebra $\mathfrak{g}$ is said to be *simple* if it has no nonzero ideals other than $\mathfrak{g}$.

It is clear that a nontrivial simple Abelian Lie algebra is necessarily one-dimensional and that a non-Abelian simple Lie algebra is semisimple.

It can be shown that the *Lie algebra* $\mathfrak{sl}(n)$ *is simple.* The corresponding calculations are quite tedious, so we restrict ourselves to the only case we need, that of $n = 2$.

The Lie algebra $\mathfrak{sl}(2)$ is three-dimensional and the matrices

$$H = E_{11} - E_{22}, \quad E_1 = E_{12}, \quad E_{-1} = E_{21}$$

constitute its basis. A straightforward calculation shows that

$$[H, E_1] = 2E_1, \quad [H, E_{-1}] = -2E_{-1}, \quad [E_1, E_{-1}] = H,$$

from which it follows in particular that the ideal $\mathfrak{a}$ of $\mathfrak{sl}(2)$ containing at least one of the elements H, E_1, E_{-1} contains all of them and so coincides with the entire algebra $\mathfrak{sl}(2)$. On the other hand, if $A = aH + a_1E_1 + a_{-1}E_{-1} \in \mathfrak{a}$, then $[H, A] = 2a_1E_1 - 2a_{-1}E_{-1} \in \mathfrak{a}$ and hence

$$aH + 2a_1E_1 = A + \frac{[H, A]}{2} \in \mathfrak{a}$$

and therefore $[H, aH + 2a_1E_1] = 4a_1E_1 \in \mathfrak{a}$. Consequently, if $\mathfrak{a} \neq \mathfrak{sl}(n)$, then $a_1 = 0$ and hence $aH \in \mathfrak{a}$, which is possible for $\mathfrak{a} \neq \mathfrak{sl}(n)$ only when $a = 0$. Therefore $A = a_{-1}E_{-1} \in \mathfrak{a}$, from which it again follows that either $\mathfrak{a} =$

$\mathfrak{gl}(n)$ or $a_{-1} = 0$. Thus if $\mathfrak{a} \neq \mathfrak{gl}(n)$, then $A = 0$, i.e. $\mathfrak{a} = 0$. □

A connected Lie group G is said to be *simple* if its Lie algebra is non-Abelian and simple or, equivalently, if any invariant subgroup of it other than G is zero-dimensional (and hence if it is closed, it is discrete). Thus if the group G is simple, then either any epimorphism $G \to G'$ is a group covering (a local isomorphism) or the group G' is trivial (consists of only the identity). The group G' is also simple, for by definition a Lie group is simple or otherwise not simple simultaneously with all the groups locally isomorphic to it.

An example of a simple Lie group is the group SL (2) as well as its universal covering group $\widetilde{\mathrm{SL}(2)}$.

Similarly, a connected Lie group is said to be *semisimple* if its Lie algebra is semisimple.

Note that any simple Lie group is semisimple.

Recall that a *commutant* $[G, G]$ of a group G is the subgroup of G generated by all the elements of the form $aba^{-1}b^{-1}$. A group G is said to be a *Cain group** if $[G, G] = G$. It follows immediately from Proposition 2 of Lecture 4 that a *connected Lie group G is a Cain group if and only if for its Lie algebra $\mathfrak{g}$ we have $\mathfrak{g} = \mathfrak{g}^2$.*

It follows in particular that *any semisimple Lie group is a Cain group.*

For example, the group SL (2) and any Lie group locally isomorphic to it, say, the group $\widetilde{\mathrm{SL}(2)}$, are Cain Lie groups.

As is immediate from the theorem on the determinant of a matrix product, *any Cain (and in particular any semisimple) matrix Lie group is unimodular*, i.e. consists of unimodular matrices. Besides, it is obvious that *any factor group of a Cain group is also a Cain group.*

Let $\mathfrak{g}$ be a linear Lie algebra over the field $\mathbb{C}$, consisting of linear operators acting in a finite-dimensional complex vector space $\mathscr{V}$ a linear operator A (not in general in $\mathfrak{g}$) is commutative with all the operators in $\mathfrak{g}$, then its kernel Ker A and image Im A are invariant under those operators

* The group derives its name from the fact that the Abelian group structure is annihilated in it. Thus the story repeats itself even in pure mathematics.

and therefore if $\mathfrak{g}$ is irreducible, then either $A = 0$ or A is nonsingular. For any eigenvalue λ of A the operator $A - \lambda E$ is singular and also commutative with all the operators in $\mathfrak{g}$. Therefore $A - \lambda E = 0$. This proves that the *only operators commutative with all the elements of an irreducible linear Lie algebra* $\mathfrak{g}$ *over the field* $\mathbb{C}$ *are scalar operators of the form* λE.

This statement is known as *Schur's lemma*. Note that nowhere in its proof have we used the algebraic structure of a Lie algebra $\mathfrak{g}$. Therefore Schur's lemma holds for any irreducible (i.e. having no nontrivial invariant subspaces) families $\mathfrak{g}$ of linear operators over the field of complex number $\mathbb{C}$.

Consider now a linear Lie algebra $\mathfrak{g}$ over $\mathbb{R}$ which consists of linear operators acting in a real vector space $\mathscr{V}$. To exploit Schur's lemma we go over from the algebra $\mathfrak{g}$ to its complexification $\mathfrak{g}^{\mathbb{C}}$ consisting of matrices (linear operators) of the form $A + iB$, $A, B \in \mathfrak{g}$, and acting in the complexification $\mathscr{V}^{\mathbb{C}}$ of $\mathscr{V}$. Clearly, if a Lie algebra $\mathfrak{g}$ (over $\mathbb{R}$) is semisimple, then the Lie algebra $\mathfrak{g}^{\mathbb{C}}$ (over $\mathbb{C}$) is also semisimple. But if $\mathfrak{g}^{\mathbb{C}}$ is semisimple, then by the Weyl theorem (Proposition 3 of Lecture 19) the space $\mathscr{V}^{\mathbb{C}}$ decomposes into a direct sum of invariant subspaces $\mathscr{V}_i$, $i = 1, \ldots, s$, in each of which the algebra $\mathfrak{g}^{\mathbb{C}}$ acts in an irreducible way. In matrix terms this means that (with a suitable choice of basis of $\mathscr{V}^{\mathbb{C}}$) every matrix in $\mathfrak{g}^{\mathbb{C}}$ (and hence in $\mathfrak{g}$) is of the form

$$A_1 \oplus \ldots \oplus A_s, \tag{1}$$

the mapping $\rho_i\colon A \mapsto A_i$ being an irreducible representation of $\mathfrak{g}^{\mathbb{C}}$ in $\mathscr{V}_i$ for any $i = 1, \ldots, s$.

Keeping this in mind, suppose that $\mathfrak{g}$ is a Lie algebra of some linear (=matrix) semisimple (and hence connected) Lie group G acting in a vector space $\mathscr{V}$. The group G naturally acts also in the vector space $\mathscr{V}^{\mathbb{C}}$, all subspaces $\mathscr{V}_i$ being invariant under that action (they are invariant under operators $A \in \mathfrak{g} = \operatorname{Re} \mathfrak{g}^{\mathbb{C}}$ and hence also under all operators e^{tA}, $t \in \mathbb{R}$, generating, in view of connectedness, the group G). Therefore any element of G also admits a decomposition of

the form (1) (in general, with complex matrices $A_1, \ldots, A_s$). All matrices of the form A_i constitute some (in general, reducible and possibly trivial) group G_i which acts in the space $\mathscr{V}_i$ and is an epimorphic image of the group G.

Note that *all groups G_i are unimodular*. Indeed, being semisimple, G is a Cain group. Hence all groups G_i are Cain and therefore unimodular. □

Now let A be an element of the centre of the group G. Being commutative with every element of G, the operator A is commutative also with every element of a Lie algebra $\mathfrak{g}$ and hence with every element of the Lie algebra $\mathfrak{g}^{\mathbb{C}}$. For any $i = 1, \ldots, s$ therefore the operator $A_i\colon \mathscr{V}_i \to \mathscr{V}_i$ in decomposition (1) of A is commutative with every element of an irreducible algebra $\rho_i(\mathfrak{g}^{\mathbb{C}})$ and hence by Schur's lemma is a scalar operator of the form $\lambda_i E$, where $\lambda_i \in \mathbb{C}$. On the other hand, being an element of the group G_i, the operator A_i is unimodular. Hence $\lambda_i^{n_i} = 1$; where $n_i = \dim \mathscr{V}_i$, and so there are only a finite number ($\leqslant n_1 n_2 \ldots n_s$) of possibilities for the element A. This proves the following proposition which has been the main aim of all our reasoning:

Proposition 1. *The centre of any semisimple (and, in particular, any simple) matrix Lie group is finite.* □

It is easy to prove with the aid of this proposition that the analogue of the Ado theorem for Lie groups is *false*, i.e. *there are connected Lie groups that are isomorphic to no matrix group*. To do this it suffices to find a connected simple Lie group with an infinite centre. We show that *such a group is the universal covering group* $\widetilde{\mathrm{SL}(2)}$ *of the group* SL (2) *of unimodular matrices of the second order* (which we already know to be simple). To do this we need an explicit construction of the group $\widetilde{\mathrm{SL}(2)}$.

Somewhat forestalling the events, denote by $\widetilde{\mathrm{SL}(2)}$ a smooth manifold which is the product $\mathbb{R} \times D$ of the real line $\mathbb{R}$ and the unit disk D in the complex plane, i.e. the disk consisting of complex numbers z such that $|z| < 1$. It is easy to see that the function $z \mapsto \dfrac{1+z}{1+\bar{z}}$ effects a continuous mapping of disk D onto the circle $|w| = 1$, without point $w = -1$. For any number $z \in D$ therefore

there is only one number t, $-\pi < t < \pi$ for which

$$e^{it} = \frac{1+z}{1+\bar{z}}.$$

That number t is symbolized $\frac{1}{i}\ln\frac{1+z}{1+\bar{z}}$.

We give in the set $\widetilde{\mathrm{SL}(2)}$ a multiplication by defining it as follows:

$$(x, u)(y, v) = \left(x + y + t, \frac{u + e^{2iy}v}{e^{2iy} + u\bar{v}}\right), \tag{1}$$

$$x, y \in \mathbb{R}, \quad u, v \in D,$$

with

$$t = \frac{1}{2i}\ln\frac{1+e^{-2iy}u\bar{v}}{1+e^{2iy}\bar{u}v}.$$

Since $|e^{2iy} + u\bar{v}|^2 - |u + e^{2iy}v|^2 = (1-|u|^2)(1-|v|^2) > 0$, we have

$$\left|\frac{u + e^{2iy}v}{e^{2iy} + u\bar{v}}\right| < 1$$

and hence formula (1) correctly defines in $\widetilde{\mathrm{SL}(2)}$ a multiplication.

That multiplication has an identity (0, 0), and for any element (x, u) there is an inverse element

$$(x, u)^{-1} = (-x, -e^{2ix}u).$$

In addition, as is shown by an easy, although lengthy, calculation, multiplication (1) is associative. Since the multiplication is obviously smooth, this proves that under multiplication (1) the *manifold* $\widetilde{\mathrm{SL}(2)}$ *is a Lie group.*

The centre of the group consists of elements (x, u) such that

$$\frac{u + e^{2iy}v}{e^{2iy} + u\bar{v}} = \frac{v + e^{2ix}u}{e^{2ix} + v\bar{u}}$$

for any y and v. In particular, when $v = 0$ there must be $u = e^{2iy}u$ for any y, which is possible only when $u = 0$. Hence $v = e^{2ix}v$ for any v, which is possible only when $x = \pi n$, where n is an integer. Conversely, it is clear that

all elements of the form $(\pi n, 0)$ are in the centre of the group $\widetilde{\mathrm{SL}\,(2)}$. Hence *the centre of the group* $\widetilde{\mathrm{SL}\,(2)}$ *is infinite.*

It now remains to be established that the group $\widetilde{\mathrm{SL}\,(2)}$ is indeed the universal covering group of SL (2). To this end we consider the mapping $\widetilde{\mathrm{SL}\,(2)} \to \mathrm{SL}\,(2)$ associating an element $(x, u) \in \widetilde{\mathrm{SL}\,(2)}$ with a matrix

$$\frac{1}{\sqrt{1-|u|^2}}\begin{pmatrix} \cos x + |u| \cos(x+\varphi) & |u| \sin(x+\varphi) - \sin x \\ |u| \sin(x+\varphi) + \sin x & \cos x - |u| \cos(x+\varphi) \end{pmatrix},$$

where $\varphi = \arg u$.

An elementary, but unfortunately rather lengthy, calculation shows that that mapping is defined correctly, that it is a homomorphism and that its kernel consists of elements of the form $(2\pi n, 0)$ and is hence discrete. Since $\dim \widetilde{\mathrm{SL}\,(2)} = \dim \mathrm{SL}\,(2) = 3$, it follows from Lemma 1 of Lecture 13 that the *homomorphism* $\widetilde{\mathrm{SL}\,(2)} \to \mathrm{SL}\,(2)$ *is a group covering.*

Since the group $\widetilde{\mathrm{SL}\,(2)}$ is obviously simply connected (the manifolds $\mathbb{R}$ and D are simply connected, and hence so is their product $\mathbb{R} \times D = \widetilde{\mathrm{SL}\,(2)}$), this completes the proof. $\square$

Explanation. In conclusion we explain the genesis of the presented construction of the group $\widetilde{\mathrm{SL}\,(2)}$ (although the proof is already formally complete).

By the theorem on polar factorization (see II, 21, Proposition 4) any unimodular matrix $A \in \mathrm{SL}\,(2)$ is uniquely decomposed into the product UP of a rotation matrix U and a positive definite unimodular matrix P. The matrix U is given by an angle of rotation x and the matrix P having the form

$$\begin{pmatrix} a & b \\ b & c \end{pmatrix},$$

where $a > 0$ and $ac - b^2 = 1$, is given by numbers $a > 0$ and b, i.e. by a complex number $z = a + ib$ in the right half-plane $a > 0$. Going over from the right half-plane to the unit circle via linear fractional transformation we thus find that every matrix $A \in \mathrm{SL}\,(2)$ is uniquely characterized

by a pair (x, u) (so that the group SL (2) is diffeomorphic to the product $S^1 \times D$), and it is the multiplication of pairs given by formula (1) that turns out to correspond to matrix multiplication. For the group $\widetilde{\text{SL (2)}}$ to be obtained it now remains to consider x not as an angle but as a point in $\mathbb{R}$.

Remark 1. The infinity of the centre of the simply connected covering group SL (2) can be proved without relying on its explicit description on the basis of general considerations. Indeed, since for any connected Lie group G its fundamental group $\pi_1\overline{G}$ is in the centre of the simply connected covering group G, for the infinity of the centre of $\widetilde{\text{SL (2)}}$ to be proved it suffices to prove that the group π_1 SL (2) is infinite. To do this we can use the refinement of Proposition 8 of Lecture 12 relating to the case, where by hypotheses, the group G contains a subset P (obviously homeomorphic to the quotient manifold G/H) such that any element $g \in G$ can be uniquely represented as $g = hp$, where $h \in H$, $p \in P$, and saying that in this case the *group* $\pi_1 H$ *is isomorphic to* $\pi_1 G$. By the theorem on polar factorization for the subgroup SO (n) of the group SL (n), $n \geqslant 2$, such a set P is the set of all unimodular positive definite $n \times n$ matrices. It can be easily shown (we have done this above for $n = 2$) that that set is homeomorphic to an open sphere in the Euclidean space $\left(\text{of dimension } N = \frac{n(n+1)}{2} - 1\right)$ and is therefore simply connected. Hence the group π_1 SL (n) is isomorphic to π_1 SO (n), and therefore for $n = 2$ it is an infinite cyclic group. We have preferred to give a straightforward, computational proof, since the explicit form of the group $\widetilde{\text{SL (2)}}$ is of independent interest as well.

We now discuss the question of geometrical motivations of the formal algebraic constructions of Lecture 19.

Recall that a *differential form* ω *of degree* m on a smooth manifold M is a (smooth) field of skew-symmetric $(m, 0)$-tensors. In local coordinates $x^1, \ldots, x^n$ every such form ω is expressed on M as

$$\omega = f_{i_1 \ldots i_m} dx^{i_1} \wedge \ldots \wedge dx^{i_m},$$

where $f_{i_1 \ldots i_m}$ are smooth functions in the corresponding coordinate neighbourhood U which are skew-symmetrically

dependent on the indices $i_1, \ldots, i_m$ and $dx^1, \ldots, dx^n$ are forms in U of degree 1 whose values $(dx^1)_a, \ldots, (dx^n)_a$ at every point $a \in U$ (that are covectors of the tangent space $\mathsf{T}_a(M)$) make up a basis conjugate to the basis $\left(\frac{\partial}{\partial x^1}\right)_a, \ldots, \left(\frac{\partial}{\partial x^n}\right)_a$ of $\mathsf{T}_a(M)$.

The collection $\Omega^m(M)$ of all differential forms of degree $m \geqslant 0$ on the manifold M is an (infinite) vector space over the field $\mathbb{R}$.

Forms of degree 0 are identified in a natural way with smooth functions on M and hence the vector space $\Omega^0(M)$ is identified with the algebra $\mathcal{F}(M)$ of smooth functions on M.

The formula

$$(\varphi \wedge \psi)_a = \varphi_a \wedge \psi_a,$$

where a is a point of M and φ and ψ are differential forms on M, correctly defines on M a differential form $\varphi \wedge \psi$ which is called the *external product* of the forms φ and ψ. The degree of $\varphi \wedge \psi$ is the sum of the degrees of φ and ψ.

The external product is associative and skew-symmetric (if p and q are the degrees of φ and ψ, then $\psi \wedge \varphi = (-1)^{pq}\, \varphi \wedge \psi$) and, for forms of degree 0, it coincides with the product of functions.

For every smooth mapping $f\colon M \to N$ the formula

$$(f^*\omega)_a(A_1, \ldots, A_m) = \omega_{f(a)}((df)_a A_1, \ldots, (df)_a A_m),$$

where $a \in M$, $A_1, \ldots, A_m \in \mathsf{T}_a(M)$ and $\omega \in \Omega^m(N)$, defines a differential form $f^*\omega \in \Omega^m(M)$.

For any function $f \in \mathcal{F}(M)$ the formula

$$(df)_a(A) = Af,$$

where $a \in M$ and $A \in \mathsf{T}_a(M)$, defines on M a differential form df of degree 1. The form is called the *differential* of f and is given in local coordinates by

$$df = \frac{\partial f}{\partial x^i}\, dx^i.$$

The operation d is uniquely extended to a linear (over $\mathbb{R}$) mapping

$$d\colon \Omega^m(M) \to \Omega^{m+1}(M)$$

defined for any $m \geqslant 0$ and having the following three properties:

(i) the mapping d is a differentiation with respect to the external product, i.e. for any forms φ and ψ it satisfies the relation

$$d(\varphi \wedge \psi) = d\varphi \wedge \psi + (-1)^m \varphi \wedge d\psi,$$

where m is the degree of φ;

(ii) there is an identity

$$d \circ d = 0,$$

i.e. $d(d\omega) = 0$ for any form ω.

(iii) for any smooth mapping $F: M \to N$ and any form $\omega \in \Omega^m N$

$$dF^*\omega = F^*d\omega.$$

It follows from these properties that in local coordinates the operator d is given by

$$(2) \qquad d\omega = df_{i_1 \ldots i_m} \wedge dx^{i_1} \wedge \ldots \wedge dx^{i_m},$$

which proves its uniqueness. To prove existence we should take formula (2) as the definition and verify that the same differential form results at the intersection of any two coordinate neighbourhoods.

The form $d\omega$ is called the *external differential* of ω.

A form $\omega \in \Omega^m(M)$ is said to be *closed* if $d\omega = 0$ and *exact* if there is a form $\varphi \in \Omega^{m-1}(M)$ such that $d\varphi = \omega$. By property (ii) of the operator d the vector space $B^m(M)$ of exact forms is contained in the vector space $Z^m(M)$ of closed forms and so a factor space

$$H^m(M) = Z^m(M)/B^m(M)$$

is defined. This is called the *space* (or *group*) *of de Rham cohomologies* of a smooth manifold M.

To relate this analytic-geometrical construction to the formal algebraic constructions of Lecture 19 recall that with respect to the Lie bracket, the vector space $\mathfrak{a}(M)$ of vector fields on the manifold M is an (infinite-dimensional) Lie algebra and the vector space $\mathcal{F}(M)$ of smooth functions on M is a module over the Lie algebra $\mathfrak{a}(M)$ (by definition $[X, Y]f = X(Yf) - Y(Xf)$ for any function $f \in \mathcal{F}(M)$).

Therefore we can introduce a vector space of cochains $C^m(\mathfrak{a}(M), \mathscr{F}(M))$ (whose definition makes sense in the infinite case as well).

By the formula

$$u(X_1, \ldots, X_m)(a) = \omega_a((X_1)_a, \ldots, (X_m)_a), \quad a \in M,$$

where $X_1, \ldots, X_m$ are arbitrary vector fields on M, any differential form $\omega \in \Omega^m(M)$ defines a cochain $u \in C^m(\mathfrak{a}(M), \mathscr{F}(M))$. Clearly, the correspondence $\omega \mapsto u$ is injective and so we can identify differential forms ω with the corresponding cochains (and denote them by the same letters).

By virtue of this identification the operator d will be defined by

$$\begin{aligned}(3)\quad (m+1)(d\omega)(X_1, \ldots, X_{m+1}) &= \sum_{i=1}^{m+1}(-1)^{i+1}X_i\omega(X_1, \ldots, \hat{X}_i, \ldots, X_{m+1}) \\ &+ \sum_{i=1}^{m}\sum_{j=i+1}^{m+1}(-1)^{i+j}\omega([X_i, X_j], \\ &\qquad X_1, \ldots, \hat{X}_i, \ldots, \hat{X}_j, X_{m+1}),\end{aligned}$$

where $X_1, \ldots, X_{m+1}$ are fields in $\mathfrak{a}(M)$, i.e. will coincide (accurate to an inessential factor $m+1$) with the operator δ for cochains (the easiest way to prove this is to verify through direct calculation that the operator d defined by formula (3) has properties (i) and (ii) and coincides on functions with their differential).

This explains the origin of the operator δ. (Note that by no means any chain u is obtained from a differential form: it is necessary and sufficient for this that for any vector fields $X_1, \ldots, X_m, Y_1, \ldots, Y_m$ and any point $a \in M$ equations $(X_1)_a = (Y_1)_a, \ldots, (X_m)_a = (Y_m)_a$ should yield $(X_1, \ldots, X_m)(a) = u(Y_1, \ldots, Y_m)(a)$. Therefore although the embedding $\Omega^m(M) \subset C^m(\mathfrak{a}(M), \mathscr{F}(M))$ does induce some homomorphism

$$(4)\qquad H^m(M) \to H^m(\mathfrak{a}(M), \mathscr{F}(M)),$$

in general that homomorphism is not an isomorphism.)

A topological interpretation of spaces $H^m(\mathfrak{g}; \mathscr{V})$ is also possible for finite-dimensional Lie algebras $\mathfrak{g}$ (over the field $\mathbb{R}$). For simplicity we restrict our discussion to the case $\mathscr{V} = \mathbb{R}$.

The form ω on a Lie group G is said to be *left-invariant* if $L_a^*\omega = \omega$ for every element $a \in G$.

All left-invariant forms of degree m make up a subspace $\Omega^m_{\text{inv}}(G)$ of the vector space $\Omega^m(G)$, which is closed under the operator d (if $\omega = L_a^*\omega$, then $d\omega = dL_a^*\omega = L_a^*d\omega$). We set

$$H^m_{\text{inv}}(G) = Z^m_{\text{inv}}(G)/B^m_{\text{inv}}(G),$$

where $Z^m_{\text{inv}}(G)$ is the space of all closed left-invariant forms of degree m and $B^m_{\text{inv}}(G)$ is its subspace consisting of forms $d\omega$, $\omega \in \Omega^{m-1}_{\text{inv}}(G)$.

Suppose as always that e is the identity of a Lie group G. Since the vector space $\mathsf{T}_eG = \mathfrak{g}$ is a Lie algebra, the skew-symmetric multilinear functionals on $\mathsf{T}_eG = \mathfrak{g}$ are nothing that cochains of that Lie algebra over a trivial $\mathfrak{g}$-module $\mathbb{R}$. Therefore $\omega \mapsto \omega_e$ yields a linear mapping

$$\Omega^m_{\text{inv}}(G) \to C^m(\mathfrak{g}; \mathbb{R}). \tag{5}$$

Proposition 2. *Mapping (5) is an isomorphism.*

Proof. A form $\omega \in \Omega^m(G)$ is left-invariant (is in $\Omega^m_{\text{inv}}(G)$) if and only if

$$\omega_a(A_1, \ldots, A_m) = u((dL_a - 1)_a A_1, \ldots, (dL_a - 1)_a A_m) \tag{6}$$

for any point $a \in G$ and any vectors $A_1, \ldots, A_m \in \mathsf{T}_aG$, where $u = \omega_e$. Thus if $\omega_e = 0$, then $\omega = 0$.

Conversely, a straightforward verification shows that for any cochain $u \in C^m(\mathfrak{g}; \mathbb{R})$ formula (6) defines a left-invariant form $\omega \in \Omega^m_{\text{inv}}(G)$ for which $\omega_e = u$. □

Thus by Proposition 2 we can identify left-invariant differential forms in $\Omega^m_{\text{inv}}(G)$ with cochains in $C^m(\mathfrak{g}, \mathbb{R})$.

By definition,

$$\omega_e(A_1, \ldots, A_m) = \omega(X_1, \ldots, X_m)(e)$$

for any form $\omega \in \Omega^m(G)$ and any vectors $A_1, \ldots, A_m \in \mathsf{T}_eG$, where $X_1, \ldots, X_m$ are vector fields with the property that $(X_1)_e = A_1, \ldots, (X_m)_e = A_m$. In particular,

it may be assumed without loss of generality that the fields $X_1, \ldots, X_m$ are left-invariant (are in the Lie algebra $\mathfrak{g} = \mathfrak{l}(G)$).

On the other hand, if the form ω is left-invariant, then the function $\omega(X_1, \ldots, X_m)$ is easily seen to be constant on G for any left-invariant vector fields $X_1, \ldots, X_m$, and hence

$$Y\omega(X_1, \ldots, X_m) = 0$$

for any vector field $Y \in \mathfrak{a}(G)$.

It follows from formula (3) that for any form $\omega \in \Omega^m_{\text{inv}}(G)$ the value $(d\omega)_e(A_1, \ldots, A_{m+1})$ of the cochain $(d\omega)_e$ on vectors $A_1, \ldots, A_{m+1} \in \mathsf{T}_eG$ is defined by the formula

$$(m+1)(d\omega)_e(A_1, \ldots, A_{m+1}) = \sum_{i=1}^{m} \sum_{j=i+1}^{m+1} (-1)^{i+j} \omega([X_i, X_j], X_1, \ldots, \hat{X}_i, \ldots, \hat{X}_j, \ldots, X_{m+1})(e),$$

where $X_1, \ldots, X_m$ are left-invariant fields on G for which $(X_1)_e = A_1, \ldots, (X_{m+1})_e = A_{m+1}$. In other words,

$$(m+1)(d\omega)_e(A_1, \ldots, A_{m+1}) = \sum_{i=1}^{m} \sum_{j=i+1}^{m+1} (-1)^{i+j} \omega_e([A_iA_j], A_1, \ldots, \hat{A}_i, \ldots, \hat{A}_j, \ldots, A_{m+1}),$$

where $[A_i, A_j]$ denotes the Lie bracket in a Lie algebra $\mathsf{T}_eG = \mathfrak{g}$ (i.e. $[A_i, A\ ] = [X_i, X_j]_e$).

This means that when left-invariant forms in $\Omega^m_{\text{inv}}(G)$ are identified with cochains in $C^m(\mathfrak{g}; \mathbb{R})$ the operator d goes over (accurate to an inessential factor $m + 1$) into an operator δ. Hence for any $m \geqslant 0$

$$H^m_{\text{inv}}(G) = H^m(\mathfrak{g}; R). \tag{7}$$

Unlike $H^m(G)$ the group $H^m_{\text{inv}}(G)$, of course, cannot be considered as a topological invariant of the smooth manifold G_{diff}. Nevertheless it can be shown that if a Lie group is connected and compact, then $H^m(G)$ and $H^m_{\text{inv}}(G)$ are isomorphic (which by virtue of (7) yields, in particular, an efficient method of calculating groups $H^m(G)$). The proof is beyond the scope of this book, however.

Lecture 21

Killing's functional of an ideal • Some properties of differentiations • The radical and nilradical of an ideal • Extension of differentiations to a universal enveloping algebra • Ideals of finite codimension of an enveloping algebra • The radical of an associative algebra • Justification of the inductive step of the construction • The proof of the Ado theorem • Conclusion

We now return to the proof of the Ado theorem. To do this we have essentially everything ready, except some purely technical lemmas, mainly on differentiations and enveloping algebras.

Let $\mathfrak{a}$ be an ideal of a Lie algebra $\mathfrak{g}$ and let $i: \mathfrak{a} \to \mathfrak{g}$ be an embedding. For any element $x \in \mathfrak{a}$ the linear operator $\operatorname{ad} i(x): \mathfrak{g} \to \mathfrak{g}$ while leaving $\mathfrak{a}$ invariant induces operators $\mathfrak{g}/\mathfrak{a} \to \mathfrak{g}/\mathfrak{a}$ and $\mathfrak{a} \to \mathfrak{a}$, the first of the operators being obviously zero and the second one coinciding with $\operatorname{ad} x: \mathfrak{a} \to \mathfrak{a}$. For any two elements $x, y \in \mathfrak{a}$ therefore the operator $\operatorname{ad} i(x) \circ \operatorname{ad} i(y)$ also induces in $\mathfrak{g}/\mathfrak{a}$ a zero operator and in $\mathfrak{a}$ an operator $\operatorname{ad} x \circ \operatorname{ad} y$. Hence $\operatorname{Tr}(\operatorname{ad} i(x) \cdot \operatorname{ad} i(y)) = \operatorname{Tr}(\operatorname{ad} x \circ \operatorname{ad} y)$, i.e. $t_{\mathfrak{g}}(i(x), i(y)) = t_{\mathfrak{a}}(x, y)$.

This means that *Killing's functional* $t_{\mathfrak{a}}$ *of the ideal* $\mathfrak{a}$ *is a restriction to* $\mathfrak{a}$ *of Killing's functional* $t_{\mathfrak{g}}$ *of the algebra* $\mathfrak{g}$.

Now let $D: \mathfrak{g} \to \mathfrak{g}$ be a differentiation of a Lie algebra $\mathfrak{g}$. We define in the direct sum $\mathfrak{g}^* = \mathfrak{g} \oplus \mathbb{K}$ an operation $[\ ,\ ]$ by the formula

$$[(x, \lambda), (y, \mu)] = ([x, y] + \lambda Dy - \mu Dx, 0),$$
$$x, y \in \mathfrak{g}, \ \lambda, \mu \in \mathbb{K}.$$

Clearly, this operation is bilinear and anticommutative. In addition, it satisfies the Jacobi identity:

$[[(x, \lambda), (y, \mu)], (z, \nu)]$

$$\begin{aligned}
&+ [[(y, \mu), (z, \nu)], (x, \lambda)] + [[(z, \nu), (x, \lambda)], (y, \mu)\\
&= ([[x, y], z] + \lambda[Dy, z] - \mu\,[Dx, z]\\
&- \nu D\,([x, y] + \lambda Dy - \mu Dx),\ 0)\\
&+ ([[y, z], x] + \mu\,[Dz, x) - \nu\,[Dy, x]\\
&- \lambda D\,([y, z] + \mu Dz - \nu Dy),\ 0)\\
&+ ([[z, x], y] + \nu\,[Dx, y] - \lambda\,[Dz, y]\\
&- \mu D\,([z, x] + \nu Dx - \lambda Dz),\ 0) = 0.
\end{aligned}$$

Thus the vector space $\mathfrak{g}^*$ is defined as a Lie algebra. By identifying every element $x \in \mathfrak{g}$ with elements $(x, 0) \in \mathfrak{g}^*$ we embed $\mathfrak{g}$ into $\mathfrak{g}^*$ as an ideal. The internal differentiation ad ξ corresponding to the element $\xi = (0, 1)$ acts on that ideal by the formula

$$(\mathrm{ad}\,\xi)\,x = [(0, 1), (x, 0)] = (Dx, 0) = Dx,$$

i.e. coincides on $\mathfrak{g}$ with a given differentiation D.

On the other hand, as applied to elements $x, y \in \mathfrak{g}$ and ξ the property that Killing's functional $t_{\mathfrak{g}^*}$ of the Lie algebra $\mathfrak{g}^*$ is invariant can be written as

$$t_{\mathfrak{g}^*}((\mathrm{ad}\ \xi)\,x,\ y) + t_{\mathfrak{g}^*}(x,\ (\mathrm{ad}\ \xi)\,y) = 0,$$

from which it follows, in view of the above discussion of Killing's functional of an ideal, that *Killing's functional of a Lie algebra* $\mathfrak{g}$ *satisfies the relation*

$$t_{\mathfrak{g}}(Dx, y) + t_{\mathfrak{g}}(x, Dy) = 0.$$

This property of Killing's functional is called a *complete invariance*.

An ideal $\mathfrak{a}$ of a Lie algebra $\mathfrak{g}$ is said to be *characteristic* if $Dx \in \mathfrak{a}$ for any element $x \in \mathfrak{a}$ and for any differentiation $D\colon \mathfrak{g} \to \mathfrak{g}$.

It follows from the property of complete invariance for Killing's functional $t_{\mathfrak{g}}$ that the *annulet* $\mathfrak{a}^{\perp}$ *with respect to* $t_{\mathfrak{g}}$ *of the characteristic ideal* $\mathfrak{a}$ *is a characteristic ideal.* Indeed, if $x \in \mathfrak{a}^{\perp}$, then $t_{\mathfrak{g}}(Dx, y) = -t_{\mathfrak{g}}(x, Dy) = 0$ for any differentiation D and for any element $y \in \mathfrak{a}$ and hence $Dx \in \mathfrak{a}^{\perp}$. □

Since the ideal $\mathfrak{g}^2$ is obviously characteristic, it follows immediately from Corollary 1 to Proposition 3 of Lecture 14 that the *radical* $\mathfrak{r}$ *of a Lie algebra* $\mathfrak{g}$ *is a characteristic ideal.*

Since every internal differentiation of a Lie algebra $\mathfrak{g}$ induces on each ideal $\mathfrak{a}$ a differentiation (no longer, in general, internal) of that ideal, *any characteristic ideal* $\mathfrak{r}$ *of the ideal* $\mathfrak{a}$ *is an ideal of the entire agebra* $\mathfrak{g}$.

In particular, an ideal of the algebra $\mathfrak{g}$ is the radical $\mathfrak{r}(\mathfrak{a})$ of the ideal $\mathfrak{a}$. Being a solvable ideal, this radical is in the radical $\mathfrak{r} = \mathfrak{r}(\mathfrak{g})$ of $\mathfrak{g}$ and hence in the intersection $\mathfrak{a} \cap \mathfrak{r}$. On the other hand, being a solvable ideal in $\mathfrak{a}$, this intersection is in $\mathfrak{r}(\mathfrak{a})$. This proves that the *radical* $\mathfrak{r}(\mathfrak{a})$ *of an ideal* $\mathfrak{a}$ *of a Lie algebra* $\mathfrak{g}$ *coincides with the intersection of that ideal with the radical* $\mathfrak{r}$ *of the entire algebra*:

$$\mathfrak{r}(\mathfrak{a}) = \mathfrak{a} \cap \mathfrak{r}.$$

Consider again the Lie algebra $\mathfrak{g}^* \supset \mathfrak{g}$ constructed above from a given differentiation $D: \mathfrak{g} \to \mathfrak{g}$. Since the radical $\mathfrak{r}$ of $\mathfrak{g}$ is in the radical $\mathfrak{r}^*$ of $\mathfrak{g}^*$, we have $D\mathfrak{r} = (\operatorname{ad} \xi)\,\mathfrak{r} \subset [\mathfrak{g}^*, \mathfrak{r}^*]$ and hence $D\mathfrak{r} \subset [\mathfrak{g}^*, \mathfrak{r}^*] \cap \mathfrak{g}$.

But by Proposition 4 of Lecture 16 the ideal $[\mathfrak{g}^*, \mathfrak{r}^*]$ of the Lie algebra $\mathfrak{g}^*$ and so the ideal $[\mathfrak{g}^*, \mathfrak{r}^*] \cap \mathfrak{g}$ of the Lie algebra $\mathfrak{g}$ are nilpotent. Thus the ideal $[\mathfrak{g}^*, \mathfrak{r}^*] \cap \mathfrak{g}$ is in the nilradical $\mathfrak{n}$ of $\mathfrak{g}$ and hence $D\mathfrak{r} \subset \mathfrak{n}$.

For convenience we formulate this statement as a separate lemma:

Lemma 1. *The image* $D\mathfrak{r}$ *of the radical of a Lie algebra* $\mathfrak{g}$ *under every differentiation* $D: \mathfrak{g} \to \mathfrak{g}$ *is in the nilradical* $\mathfrak{n}$ *of that algebra*:

$$D\mathfrak{r} \subset \mathfrak{n}. \quad \square$$

Corollary. *For any ideal* $\mathfrak{a}$ *of a Lie algebra* $\mathfrak{g}$ *its nilradical* $\mathfrak{n}(\mathfrak{a})$ *is the intersection of* $\mathfrak{a}$ *and the nilradical* $\mathfrak{n} = \mathfrak{n}(\mathfrak{g})$ of $\mathfrak{g}$:

$$\mathfrak{n}(\mathfrak{a}) = \mathfrak{a} \cap \mathfrak{n}.$$

Proof. Let $x \in \mathfrak{g}$. Then by Lemma 1 applied to a Lie algebra $\mathfrak{a}$ and to its differentiation D induced by an internal differentiation ad x we have an inclusion $[x, \mathfrak{r}(\mathfrak{a})] \subset \mathfrak{n}(\mathfrak{a})$ and hence an inclusion $[x, \mathfrak{n}(\mathfrak{a})] \subset \mathfrak{n}(\mathfrak{a})$. This means that the nilpotent subalgebra $\mathfrak{n}(\mathfrak{a})$ is an ideal of the Lie algebra $\mathfrak{g}$ and is therefore in its nilradical $\mathfrak{n}$. Thus $\mathfrak{n}(\mathfrak{a}) \subset \mathfrak{a} \cap \mathfrak{n}$. Since the inverse inclusion is obvious (the intersection $\mathfrak{a} \cap \mathfrak{n}$ is a nilpotent ideal in $\mathfrak{a}$) this proves the corollary. □

Now we discuss differentiations in connection with the universal enveloping algebra $\mathcal{U}$ of a Lie algebra $\mathfrak{g}$ (see Lecture 5).

It is clear that every differentiation D of the associative algebra $\mathcal{U}$ is also a differentiation of the corresponding commutator Lie algebra $[\mathcal{U}]$. Hence if $D\mathfrak{g} \subset \mathfrak{g}$, then D induces on $\mathfrak{g}$ some differentiation $D\colon \mathfrak{g} \to \mathfrak{g}$ of the Lie algebra $\mathfrak{g}$. Can any differentiation $D\colon \mathfrak{g} \to \mathfrak{g}$ be obtained in this way, that is, can it be extended to some differentiation $D\colon \mathcal{U} \to \mathcal{U}$ of the associative algebra $\mathcal{U}$? The answer is found to be yes:

Lemma 2. *Any differentiation D of a Lie algebra $\mathfrak{g}$ can be uniquely extended to some differentiation (denoted by the same letter D) of a universal enveloping algebra $\mathcal{U}$.*

Proof. Since every element of $\mathcal{U}$ is a polynomial in elements of $\mathfrak{g}$, the differentiation $D\colon \mathcal{U} \to \mathcal{U}$, if it exists, is uniquely defined. Since, however, the elements in $\mathcal{U}$ can in general be defined in many different ways in terms of the elements of $\mathfrak{g}$, a direct construction of $D\colon \mathcal{U} \to \mathcal{U}$ requires a rather arduous verification of its correctness. We therefore take a roundabout way of using a technical device proposed by Jacobson.

Let $\mathcal{A}$ be an algebra of 2×2 matrices of the form

$$\begin{pmatrix} u & v \\ 0 & u \end{pmatrix},$$

where $u, v \in \mathcal{U}$. Consider a mapping

$$\varphi : x \mapsto \begin{pmatrix} x & Dx \\ 0 & x \end{pmatrix}$$

of a Lie algebra $\mathfrak{g}$ into $\mathcal{A}$, where D is a given differentiation of $\mathfrak{g}$. Since

$$\begin{pmatrix} x & Dx \\ 0 & x \end{pmatrix}\begin{pmatrix} y & Dy \\ 0 & y \end{pmatrix}-\begin{pmatrix} y & Dy \\ 0 & y \end{pmatrix}\begin{pmatrix} x & Dx \\ 0 & x \end{pmatrix}$$

$$=\begin{pmatrix} xy-yx & x\cdot Dy+Dx\cdot y-y\cdot Dx-Dy\cdot x \\ 0 & xy-yx \end{pmatrix}$$

$$=\begin{pmatrix} [x, y] & [x, Dy]+[Dx, y] \\ 0 & [x, y] \end{pmatrix}=\begin{pmatrix} [x, y] & D[x, y] \\ 0 & [x, y] \end{pmatrix},$$

the mapping φ is a homomorphism of the Lie algebra $\mathfrak{g}$ into the commutator Lie algebra $[\mathcal{A}]$. By virtue of universality, therefore, there is a homomorphism $\psi = \mathfrak{U}\varphi$ of algebra $\mathfrak{U}$ into algebra $\mathcal{A}$ such that $\varphi = \psi \circ \iota$, where $\iota\colon \mathfrak{g} \to \mathfrak{U}$ is an embedding. It is immediate from the fact that $\mathfrak{U}$ is generated by elements in $\mathfrak{g}$ that for any element $u \in \mathfrak{U}$ the matrix φu is of the form

$$\varphi u = \begin{pmatrix} u & v \\ 0 & u \end{pmatrix}, \quad \text{where } v \in \mathfrak{U}.$$

We define an (obviously linear) mapping $D\colon \mathfrak{U} \to \mathfrak{U}$ by putting $Du = v$.

Since $\psi(uv) = \psi u \cdot \psi v$ for any elements $u, v \in \mathfrak{U}$, i.e.

$$\begin{pmatrix} uv & D(uv) \\ 0 & uv \end{pmatrix}=\begin{pmatrix} u & Du \\ 0 & u \end{pmatrix}\begin{pmatrix} v & Dv \\ 0 & v \end{pmatrix}=\begin{pmatrix} uv & u\cdot Dv+Du\cdot v \\ 0 & uv \end{pmatrix},$$

the mapping $D\colon \mathfrak{U} \to \mathfrak{U}$ is a differentiation of $\mathfrak{U}$. Since it obviously extends the given differentiation D of the Lie algebra $\mathfrak{g}$, this completes the proof of Lemma 2. □

In the universal algebra $\mathfrak{U}$ we are concerned with (two-sided) ideals $\mathcal{A}$ for which the quotient algebra $\mathfrak{U}/\mathcal{A}$ is finite-dimensional. Such ideals are said to have a *finite codimension*, and we write $\operatorname{codim} \mathcal{A} < \infty$.

Recall that an element a of an associative algebra is said to be *algebraic* if there is a nonzero polynomial $p(T)$ such that $p(a) = 0$.

Also recall (see Lecture 5) that for any basis $x_1, \ldots, x_n$ of a Lie algebra $\mathfrak{g}$ (which is assumed here to be finite-dimensional) monomials of the form $x_{i_1}x_{i_2} \ldots x_{i_s}$, where $i_1 \leqslant$

$\leqslant i_2 \leqslant \ldots \leqslant i_s$, i.e. of the form $x_1^{k_1} x_2^{k_2} \ldots x_n^{k_n}$, where $k_1 \geqslant 0$, $k_2 \geqslant 0$, ..., $k_n \geqslant 0$, make up a basis of the universal algebra $\mathfrak{U}$. It follows easily that codim $\mathscr{A} < \infty$ *if and only if cosets* $\bar{x}_1 = x_1 + \mathscr{A}$, ..., $x_n = \bar{x}_n = x_n + \mathscr{A}$ *are algebraic in* $\mathfrak{U}/\mathscr{A}$. Indeed, the condition that $\bar{x}_i$ should be algebraic implies that for some $m_i \geqslant 1$ the element $\bar{x}_i^{m_i}$ is a linear combination of elements $1, \bar{x}_i, \ldots, \bar{x}_i^{m_i-1}$. Therefore if all elements $\bar{x}_1, \ldots, \bar{x}_n$ are algebraic, then any monomial of the form $\bar{x}_1^{k_1} \ldots \bar{x}_n^{k_n}$ (and hence any element of $\mathfrak{U}/\mathscr{A}$) is a linear combination of monomials for which $0 \leqslant k_i < m_i$ with any $i = 1, \ldots, n$. Since there is a finite number of monomials satisfying the last condition, this proves that $\mathfrak{U}/\mathscr{A}$ is finite-dimensional and that hence codim $\mathscr{A} < \infty$. The converse is obvious since any element of a finite-dimensional algebra is algebraic. □

Notice that the condition that $\bar{x}_i$ should be algebraic implies existence of a nonzero polynomial $p_i(T)$ such that $p_i(x_i) \in \mathscr{A}$.

Recall that a *product* $\mathscr{A}\mathscr{B}$ of two ideals $\mathscr{A}$ and $\mathscr{B}$ of an associative algebra is the span of all possible elements of the form ab, where $a \in \mathscr{A}$ and $b \in \mathscr{B}$. That product is obviously an ideal.

Lemma 3. *A product* $\mathscr{A}\mathscr{B}$ *of any two ideals* $\mathscr{A}$ *and* $\mathscr{B}$ *of finite codimension is also an ideal of finite codimension.*

Proof. If $p_i(T)$ and $q_i(T)$ are polynomials such that $p_i(x_i) \in \mathscr{A}$ and $q_i(x_i) \in \mathscr{A}$, then polynomials $r_i(T) = p_i(T)\, q_i(T)$ have the property that $r_i(x_i) \in \mathscr{A}$. □

We also need the simplest facts about nilpotent ideals in associative algebras.

In accordance with the general terminology of algebra theory, an ideal $\mathscr{A}$ of an associative algebra $\mathscr{V}$ is said to be *nilpotent* if there is $k \geqslant 0$ such that the product of any k elements of $\mathscr{A}$ is zero, i.e. in other words if $\mathscr{A}^k$ is a zero ideal. Obviously the sum of any two nilpotent ideals is a nilpotent ideal, from which it follows that in any finite-dimensional associative algebra $\mathscr{V}$ there is a maximal nilpotent ideal $\mathscr{R}$ which contains any other nilpotent ideal. That maximal ideal is called the *radical* of the associative algebra $\mathscr{V}$.

An ideal $\mathscr{A}$ of $\mathscr{V}$ is said to be a *nilideal* if it consists of nilpotent elements. Clearly, any nilpotent ideal is a nilideal. It turns out that, conversely, *any nilideal $\mathscr{A}$ of a finite-dimensional associative algebra $\mathscr{V}$ is nilpotent* (and is therefore in its radical $\mathscr{R}$). Indeed, since the ideal $\mathscr{A}$ (or more precisely its commutator algebra $[\mathscr{A}]$) is a subalgebra of the commutator Lie algebra $[\mathscr{V}]$, Proposition 3 of Lecture 17 is applicable to it. □

The sum $a + b$ of two nilpotent elements is in general not a nilpotent element. It is a different matter if one of the elements is in the radical.

Lemma 4. *If $a \in \mathscr{R}$, then for any nilpotent element b the sum $a + b$ is nilpotent.*

Proof. Use Proposition 3* of Lecture 17 (notice that up to this point it has been enough to refer to Proposition 3), taking as $\mathscr{Q}$ the vector subspace of the algebra $\mathscr{V}$, generated by the radical $\mathscr{R}$ and an element b, and as $\mathfrak{g}$ the union of $\mathscr{R}$ and b (since $[\mathscr{R}, b] \subset \mathscr{R}$, the set $\mathfrak{g}$ is closed under commutation). By this proposition the subspace $\mathscr{Q}$ is associatively nilpotent. Therefore, in particular, its element $a + b$ is nilpotent. □

In the following lemma it is no longer enough to refer to Proposition 3* of Lecture 17 and one has to partially return to its proof.

Lemma 5. *Suppose that a finite-dimensional associative algebra $\mathscr{V}$ is generated by a subalgebra $\mathfrak{h}$ of its commutator Lie algebra $[\mathscr{V}]$. Then every ideal $\mathfrak{n}$ of the algebra $\mathfrak{h}$, which consists of nilpotent elements of $\mathscr{V}$, is in the radical $\mathscr{R}$ of $\mathscr{V}$.*

Proof. It suffices to prove that the ideal $\mathscr{N}$ of $\mathscr{V}$ generated by $\mathfrak{n}$ is nilpotent. Since $\mathfrak{h}$ generates $\mathscr{V}$, any element in $\mathscr{N}$ is a linear combination of products of elements in the ideal $\mathfrak{n}$ and in the algebra $\mathfrak{h}$. The *rank* of every such product is the number of factors in $\mathfrak{n}$. If the product contains a factor of the form ax, where $a \in \mathfrak{n}$ and $x \in \mathfrak{g}$, then using the formula $ax = [a, x] + xa$ we can represent it as a sum of two products of the same rank in which either the number of factors in $\mathfrak{g}$ is less by one or one of the factors is shifted to the left. Any product of rank r therefore can be represented as a sum of products of the form ab, where a is a product (possibly empty) of elements in $\mathfrak{g}$ and b is a product of r elements in $\mathfrak{n}$. By Proposition 3 of Lecture 16 a Lie nilsubal-

gebra $\mathfrak{n}$ is associatively nilpotent, i.e. there is a number n such that any product of $r \geqslant n$ elements in $\mathfrak{n}$ is zero. Therefore any element of $\mathscr{N}$ which is a linear combination of products of rank $\geqslant n$ is zero. Since every element of the ideal $\mathscr{N}^n \subset \mathscr{N}$ has by definition that property, this proves that $\mathscr{N}^n = 0$, i.e. that the ideal $\mathscr{N}$ is nilpotent. □

Now we are ready to proceed directly to the proof of the Ado theorem. That proof is based on an inductive construction which is made possible by the following lemma:

Lemma 6. *Let*

$\mathfrak{g}$ *be a finite-dimensional solvable Lie algebra;*

$\mathfrak{n}$ *be its radical;*

$\mathfrak{U}$ *be the universal enveloping algebra of* $\mathfrak{g}$;

$\mathscr{A}$ *be an ideal of finite codimension of* $\mathfrak{U}$ *such that for any element* $x \in \mathfrak{n}$ *the coset* $x + \mathscr{A}$ *is a nilpotent element of the quotient algebra* $\mathfrak{U}/\mathscr{A}$.

Then there is an ideal $\mathscr{B}$ *in* $\mathfrak{U}$, *such that*:

(a) $\mathscr{B} \subset \mathscr{A}$;

(b) codim $\mathscr{B} < \infty$;

(c) *for any element* $x \in \mathfrak{n}$ *the coset* $x + \mathscr{B}$ *is a nilpotent element of* $\mathfrak{U}/\mathscr{B}$;

(d) *every differentiation* D *of* $\mathfrak{U}$ *sending* $\mathfrak{g}$ *to itself sends* $\mathscr{B}$ *to itself.*

Proof. Since any homomorphism of associative algebras is also a homomorphism of the corresponding commutator algebras, the image

$$\mathfrak{h} = (\mathfrak{g} + \mathscr{A})/\mathscr{A}$$

of the Lie algebra $\mathfrak{g}$ in the algebra $\mathscr{V} = \mathfrak{U}/\mathscr{A}$ is a subalgebra of the commutator Lie algebra $[\mathscr{V}]$ generating $\mathscr{V}$. Therefore since by hypothesis the image $(\mathfrak{n} + \mathscr{A})/\mathscr{A}$ of the ideal $\mathfrak{n}$ in $\mathscr{V}$ consists of nilpotent elements, by Lemma 4 that image is in the radical $\mathscr{R}$ of $\mathscr{V}$. Hence so is the ideal of $\mathscr{V}$ generated by the image. Consequently this ideal is nilpotent. Since this last ideal is of the form $\mathscr{C}/\mathscr{A}$, where $\mathscr{C}$ is an ideal in $\mathfrak{U}$ generated by $\mathfrak{n}$ and $\mathscr{A}$, this proves that there is a number r such that the ideal $\mathscr{B} = \mathscr{C}^r$ is in $\mathscr{A}$, i.e. has property (a). By Lemma 3 $\mathscr{B}$ has also property (b). Since for any $x \in \mathfrak{n}$ there is by hypothesis a number $s \geqslant 0$ such that $x^s \in \mathscr{A} \subset \mathscr{C}$, we have $x^{sr} \in \mathscr{C}^r = \mathscr{B}$ and so the element $x + \mathscr{B}$ of $\mathfrak{U}/\mathscr{B}$ is nilpotent. Thus $\mathscr{B}$ has also property (c).

Finally by Lemma 1 every differentiation D of $\mathfrak{z}$ has the property that $D\mathfrak{z} \subset \mathfrak{n}$. Therefore if the differentiation D of $\mathcal{U}$ sends $\mathfrak{z}$ to $\mathfrak{z}$, then in fact it sends $\mathfrak{z}$ to $\mathfrak{n}$ and hence the entire algebra $\mathcal{U}$ to its ideal generated by $\mathfrak{n}$. Consequently, all the more so $D\mathcal{U} \subset \mathscr{C}$ and therefore $D(\mathcal{U}^r) \subset \mathscr{C}^r = \mathscr{B}$. Then $D(\mathscr{B}) = D(\mathscr{C}^r) \subset D(\mathcal{U}^r) \subset \mathscr{B}$, which proves property (d). □

A representation ρ of a Lie algebra $\mathfrak{g}$ is said to be a *nilrepresentation* if for any element $x \in \mathfrak{n}$ of the nilradical $\mathfrak{n}$ of $\mathfrak{g}$ the operator $\rho(x)$ is nilpotent.

Proposition 2 (the inductive step of the construction). *Let a Lie algebra* $\mathfrak{n}$ *be decomposed into a direct sum*

$$\mathfrak{g} = \mathfrak{z} \oplus \mathfrak{h}$$

of a solvable ideal $\mathfrak{z}$ *and a subalgebra* $\mathfrak{h}$. *Then for any finite-dimensional nilrepresentation* σ *of the algebra* $\mathfrak{z}$ *there is a representation* ρ *of* $\mathfrak{g}$ *such that*

$$\bigcap \operatorname{Ker} \rho \subset \operatorname{Ker} \sigma.$$

If the Lie algebra $\mathfrak{g}$ *is nilpotent or if on the contrary its nilradical coincides with the nilradical of the algebra* $\mathfrak{z}$, *then* ρ *can be chosen from among nilrepresentations.*

Proof. Consider an element $x = y + z$, $y \in \mathfrak{z}$, $z \in \mathfrak{h}$ of $\mathfrak{g}$. Its component y defines by the formula $L_y\colon a \mapsto ya$, $a \in \mathcal{U}$, a shift left $L_y\colon \mathcal{U} \to \mathcal{U}$ of the universal enveloping algebra $\mathcal{U}$ of the Lie algebra $\mathfrak{z}$ while z defines a differentiation D_z of $\mathfrak{z}$ which is by definition an extension of the differentiation $\operatorname{ad} z$ of $\mathfrak{z}$. We define a mapping $\bar{\rho}$ of the algebra $\mathfrak{g}$ into the algebra $\operatorname{End} \mathcal{U}$ of linear operators $\mathcal{U} \to \mathcal{U}$ by the formula

$$\bar{\rho}(x) = L_y + D_z.$$

Let $x_1 = y_1 + z_1$ be another element of $\mathfrak{g}$. Since

$$\begin{aligned}[x, x_1] &= [y, y_1] + [y, z_1] + [z, y_1] + [z, z_1] \\ &= ([y, y_1] - D_{z_1} y + D_z x_1) + [z, z_1],\end{aligned}$$

we have

$$\bar{\rho}([x, x_1]) = L_{[y, y_1]} - L_{D_z y} + L_{D_z x_1} + D_{[z, z_1]}.$$

On the other hand,

$$[\bar{\rho}(x), \bar{\rho}(x_1)] = [L_y + D_z, L_{y_1} + D_{z_1}]$$
$$= [L_y, L_{y_1}] + [D_z, L_{y_1}] + [L_y, D_{z_1}] + [D_z, D_{z_1}],$$

with

$$[L_y, L_{y_1}] = L_y L_{y_1} - L_{y_1} L_y = L_{yy_1} - L_{y_1 y} = L_{[y, y_1]}.$$

Since, however, the differentiation $D_{[z_1, z_2]}$ coincides on $\mathfrak{z}$ with the differentiation ad $[z, z_1] = [\text{ad } z, \text{ad } z_1]$ and D_z and D_{z_1} coincide with ad z and ad z_1, we have

$$[D_z, D_{z_1}] = D_{[z_1, z_2]}$$

on $\mathfrak{z}$ and therefore everywhere on $\mathcal{U}$.

Moreover, since for any element $a \in \mathcal{U}$

$$[D_z, L_{y_1}]\, a = D_z L_{y_1} a - L_{y_1} D_z a$$
$$= D_z (y_1 a) - y_1 D_z a = D_z y_1 \cdot a,$$

we have

$$[D_z, L_{y_1}] = L_{D_z y_1}.$$

Similarly

$$[D_{z_1}, L_y] = L_{D_{z_1} y}.$$

This proves that

$$\bar{\rho}([x, x_1]) = [\bar{\rho}(x), \bar{\rho}(x_1)],$$

i.e. that $\bar{\rho}$ is a homomorphism (an "infinite-dimensional representation") of the Lie algebra $\mathfrak{g}$ into the commutator Lie algebra of linear operators $\mathcal{U} \to \mathcal{U}$. Notice that that homomorphism is defined only by the decomposition $\mathfrak{g} = \mathfrak{z} \oplus \mathfrak{h}$ and does not depend on a given representation σ.

Now let us consider the representation σ. Using the universality of the algebra $\mathcal{U}$ we can extend this representation to some homomorphism (which we denote by the same symbol σ) of $\mathcal{U}$ into the algebra of operators acting in the space of the representation σ. Since the latter algebra is finite-dimensional, the kernel $\mathcal{A}$ of that homomorphism is of finite codimension. The condition that the representation σ is a nilrepresentation is just the same as saying that for any

element x of the nilradical $\mathfrak{n}$ of $\mathfrak{s}$ the coset $x + \mathcal{A}$ is a nilpotent element of the algebra $\mathcal{U}/\mathcal{A}$ (isomorphic to a linear algebra σ $(\mathcal{U})$. Therefore we can apply Lemma 6 to the algebra $\mathfrak{s}$ and the ideal $\mathcal{A}$. There is an ideal $\mathcal{B}$ in the algebra $\mathcal{U}$, therefore, with properties (a) to (d) of that lemma.

Since $\mathcal{B}$ is an ideal, we have $L_y(\mathcal{B}) \subset \mathcal{B}$ for any element $y \in \mathfrak{s}$ and since $\mathcal{B}$ has property (d), we have $D_z(\mathcal{B}) \subset \mathcal{B}$ for any element $z \subset \mathfrak{h}$. Therefore $\bar{\rho}(x)(\mathcal{B}) \subset \mathcal{B}$ for any element $x \in \mathfrak{g}$ and hence the formula

$$\rho(x)(u + \mathcal{B}) = \bar{\rho}(x)u + \mathcal{B}, \qquad u \in \mathcal{U},$$

correctly defines some linear operator

$$\rho(x)\colon \mathcal{U}/\mathcal{B} \to \mathcal{U}/\mathcal{B}.$$

Since the mapping $\bar{\rho}\colon x \mapsto \bar{\rho}(x)$ is a homomorphism of Lie algebras, the mapping $\rho\colon x \mapsto \rho(x)$ is also a homomorphism and hence a representation (for by property (b) the quotient algebra $\mathcal{U}/\mathcal{A}$ is finite-dimensional).

If the element x is in $\mathfrak{s}$, then $\rho(x)\, L_{\bar{x}}$, where $\bar{x} = x + \mathcal{B}$. Therefore if $\rho(x) = 0$, then $L_x(\mathcal{U}) \subset \mathcal{B}$ and hence $x \in \mathcal{B}$ (recall that $\mathcal{U}$ is a unital algebra). Thus $x \in \mathcal{A}$ (property (a)) and therefore $\sigma(x) = 0$. So $\mathfrak{s} \cap \operatorname{Ker} \rho \subset \operatorname{Ker} \sigma$.

We now apply Lemma 5 to the associative algebra $\mathcal{U}/\mathcal{B}$, the Lie algebra $(\mathfrak{s} + \mathcal{B})\mathcal{B}$ and its ideal $(\mathfrak{n} + \mathcal{B})/\mathcal{B}$. This is possible since the conditions of Lemma 5 hold by virtue of properties (b) and (c). Thus by Lemma 5 every element $\bar{x} = x + \mathcal{B}$, $x \in n$, is in the radical of the associative algebra $\mathcal{U}/\mathcal{B}$ and is therefore nilpotent. So the linear operator $L_{\bar{x}}\colon \bar{a} \mapsto \overline{xa}$ is also nilpotent. Since $\rho(x) = L_{\bar{x}}$, this proves that if the nilradical of the algebra $\mathfrak{g}$ coincides with the nilradical $\mathfrak{n}$ of $\mathfrak{s}$, the representation ρ is a nilrepresentation.

It remains to consider the case where the entire algebra $\mathfrak{g}$ is nilpotent (and so in particular $\mathfrak{s} = \mathfrak{n}$). We must show that in this case the operator $\rho(x)$ is nilpotent for any element $x \in \mathfrak{g}$.

Let as above $x = y + z$, where $y \in \mathfrak{s}$, $z \in \mathfrak{h}$. Since in the case in question $\mathfrak{s} = \mathfrak{n}$, according to the foregoing, the operator $\rho(y)$ is nilpotent. Moreover, a more precise statement can be formulated by applying the same lemma 5 to a li-

near associative algebra $\mathscr{V}$ generated by operators $\rho(x)$, $x \in \mathfrak{g}$. This algebra is finite-dimensional, generated by a Lie algebra $\rho(\mathfrak{g})$ and the ideal $\rho(\mathfrak{n})$ of $\rho(\mathfrak{g})$ consists, as just said, of nilpotent elements. By Lemma 5, therefore, the operators $\rho(y)$, $y \in \mathfrak{n}$, are all in the radical $\mathfrak{R}$ of $\mathscr{V}$.

On the other hand, since the algebra $\mathfrak{g}$ is nilpotent, any operator of the form ad z, $z \in \mathfrak{h}$, is nilpotent. This means that every differentiation D_z: $\mathscr{U} \to \mathscr{U}$ restricted to $\mathfrak{s}$ is nilpotent. Since for any differentiation D, any number N and any two elements a and b

$$D^N(ab) = \sum_{i=0}^{N} \binom{N}{i} D_a^i \cdot D^N$$

it follows from $D^n a = 0$ and $D^m b = 0$ that $D^{n+m-1}(ab) = 0$. For any product $a \in \mathscr{U}$ of elements in $\mathfrak{s}$, therefore, there is $n(a)$ such that $D_z^{n(a)}(a) = 0$. Going over to the quotient algebra $\mathscr{U}/\mathscr{B}$ we get $\rho(z)^{n(a)}(\bar{a}) = 0$, where $\bar{a} = a + \mathscr{B}$. Since $\mathscr{U}/\mathscr{B}$ is finite-dimensional and has a basis $\bar{a}_1, \ldots, \bar{a}_s$ consisting of elements of the form $\bar{a}$, it follows that there is n such that $\rho(z)\mathscr{B}(\bar{a}_i) = 0$ for all elements $\bar{a}_i$, $i = 1, \ldots, n$, of that basis. But then $\rho(z)^n = 0$ on $\mathscr{U}/\mathscr{B}$, i.e. the operator $\rho(z)$ is nilpotent.

Since $\rho(x) = \rho(y) + \rho(z)$, to complete the proof of Proposition 2 it remains to apply Lemma 4. □

At last we can prove the Ado theorem, even in a somewhat stronger formulation:

Proposition 3 (Ado theorem). *For any Lie algebra $\mathfrak{g}$ there is its faithful nilrepresentation.*

Proof. We carry out a gradual, step-by-step construction of this representation.

Step 1. Let $\mathfrak{z}$ be the centre of $\mathfrak{g}$ and let $x_1, \ldots, x_m$ be its arbitrary basis. On choosing in some vector space $\mathscr{V}$ (of dimension $\geqslant m + 1$) a nilpotent operator A such that $A^{m+1} = 0$ but $A^m \neq 0$, we put

$$\rho_{\mathfrak{z}}(x) = \lambda_1 A + \ldots + \lambda_k A^k + \ldots + \lambda_m A^m$$

for any element $x = \lambda_1 x_1 + \ldots + \lambda_k x_k + \ldots + \lambda_m x_m$ of the centre $\mathfrak{z}$. Since all operators of the form $\lambda_1 A + \ldots + \lambda_m A^m$ are commutative and nilpotent and they are

nonzero when $(\lambda_1, \ldots, \lambda_m) \neq (0, \ldots, 0)$, the mapping ρ is a faithful nilrepresentation of the algebra $\mathfrak{z}$.

Step 2. Let $\mathfrak{n}$ be the nilradical of $\mathfrak{g}$. Then the quotient algebra $\mathfrak{n}' = \mathfrak{n}/\mathfrak{z}$ is also nilpotent and therefore has (by Proposition 2 of Lecture 17) a chain of ideals

$$0 = \mathfrak{n}'_0 \subset \mathfrak{n}'_1 \subset \ldots \subset \mathfrak{n}'_m = \mathfrak{n}',$$

such that $\dim \mathfrak{n}'_i = i$, for any $i = 0, 1, \ldots, m = \dim \mathfrak{n}'$ (the numbering in Proposition 2 of Lecture 17 was backward, which is of no significance of course). The inverse images of those ideals in $\mathfrak{n}$ yield an ascending chain of ideals

$$\mathfrak{z} = \mathfrak{n}_0 \subset \mathfrak{n}_1 \subset \ldots \subset \mathfrak{n}_m = \mathfrak{n}$$

which starts with the centre $\mathfrak{z}$ and is such that $\dim \mathfrak{n}_{i+1} = \dim \mathfrak{n}_i + 1$. We show by induction that for any $i = 0, 1, \ldots, m$ there is a nilrepresentation ρ_i of $\mathfrak{n}_i$ faithful on the ideal $\mathfrak{n}_0 = \mathfrak{z}$.

The beginning of induction is ensured by step 1 of the proof ($\rho_0 = \rho_{\mathfrak{z}}$). Suppose for some i a faithful nilrepresentation ρ_i on $\mathfrak{z}$ has already been constructed. On choosing in $\mathfrak{n}_{i+1}$ a subspace $\mathfrak{h}$ complementary to $\mathfrak{n}_i$ and noticing that being one-dimensional that subspace is therefore a Lie algebra we find that the conditions of Proposition 2 (with $\mathfrak{s} = \mathfrak{n}_i$ and $\sigma = \rho_i$) are satisfied. Since the ideal $\mathfrak{n}_{i+1}$ is nilpotent, by this proposition there is a nilrepresentation ρ_{i+1} of $\mathfrak{n}_{i+1}$ for which $\mathfrak{n}_i \cap \operatorname{Ker} \rho_{i+1} \subset \operatorname{Ker} \rho_i$ and which is thus as before faithful on $\mathfrak{z}$.

So when $i = m$ we obtain a nilrepresentation $\rho_{\mathfrak{n}} = \rho_{\mathfrak{m}}$ of the ideal $\mathfrak{n}$, which is faithful on the centre $\mathfrak{z}$.

Step 3. Let $\mathfrak{r}$ be the radical of a Lie algebra $\mathfrak{g}$. On considering the solvable algebra $\mathfrak{r}/\mathfrak{n}$ and using Proposition 1 of Lecture 16 we obtain in the radical $\mathfrak{r}$ by the same construction as in step 2 a chain of subalgebras

$$\mathfrak{n} = \mathfrak{r}_0 \subset \mathfrak{r}_1 \subset \ldots \subset \mathfrak{r} = \mathfrak{r}$$

beginning with $\mathfrak{n}$, such that for any $i = 0, 1, \ldots, m$ the subalgebra $\mathfrak{r}_i$ is an ideal of the subalgebra $\mathfrak{r}_{i+1}$. Here we can again apply the same inductive process starting with the representation $\rho^{\mathfrak{n}}$ of the nilradical $\mathfrak{n}$ constructed in step 2. The possibility of repeated applications of Proposi-

tion 2 is now ensured by the fact that the same ideal $\mathfrak{n}$ is the nilradical of each of the algebras $\mathfrak{r}_i$ by the corollary to Lemma 1.

As a result we obtain some nilrepresentation $\rho_{\mathfrak{r}}$ of the radical $\mathfrak{r}$, which is faithful on the centre $\mathfrak{z}$.

Step 4. In this step we apply the same Proposition 2 to the Levi decomposition

$$\mathfrak{g} = \mathfrak{r} + \mathfrak{m}$$

of the algebra $\mathfrak{g}$ and to the nilrepresentation $\rho_{\mathfrak{r}}$. Since $\mathfrak{n}(\mathfrak{r}) = \mathfrak{n}$, we obtain a nilrepresentation $\rho_{\mathfrak{g}}$ of the entire Lie algebra $\mathfrak{g}$, which is faithful on the centre of $\mathfrak{g}$.

Step 5. Consider now an adjoint representation ad and the direct sum of it and the representation $\rho_{\mathfrak{g}}$

$$\rho = \mathrm{ad} \oplus \rho_{\mathfrak{g}}.$$

Since $\mathrm{Ker\ ad} = \mathfrak{z}$ and $\mathfrak{z} \cap \mathrm{Ker}\,\rho_{\mathfrak{g}} = 0$, we have $\mathrm{Ker}\,\rho = 0$, i.e. ρ is a faithful representation. Since the representation ad is a nilrepresentation and a direct sum of two nilrepresentations is of course a nilrepresentation, this completes the proof of Proposition 3. □

Only now can we consider as proved the Cartan theorem of Lecture 10 on the equivalence of the categories of simply connected Lie groups and of real Lie algebras. It is clear why in Lecture 10 the situation with the proof of this theorem was characterized as "not satisfactory" (the second of the known proofs of the Cartan theorem is by no means simpler than the one presented since although it does not use the Ado theorem, it also relies on the Levi theorem). The search for a direct proof of the Cartan theorem is therefore a very challenging problem.

SUPPLEMENT TO THE ENGLISH TRANSLATION

(Proof of the Cartan Theorem by V. V. Gorbatsevich)

After the appearance of the Russian edition of this book V. V. Gorbatsevich communicated to me a very brief proof of the Cartan theorem in Lecture 10 which does without invoking the Ado theorem.

In that proof a Lie algebra $\mathfrak{g}$ is said to be *realizable* if there is a Lie group G whose Lie algebra is $\mathfrak{g}$.

As explained in Lecture 10, the Cartan theorem reduces to the statement that *any Lie algebra* $\mathfrak{g}$ *is realizable.* It is just in this form that we prove it.

Let $\mathfrak{z}$ be the centre of a Lie algebra $\mathfrak{g}$. We first prove that *if* $\mathfrak{z} = 0$, *then* $\mathfrak{g}$ *is realizable.* To this end we consider a homomorphism ad of $\mathfrak{g}$ into the Lie algebra of all linear operators $\mathfrak{g} \to \mathfrak{g}$. That homomorphism sends an element $a \in \mathfrak{g}$ to an operator ad a acting by the formula

$$(\mathrm{ad}\ a)\, x = [a, x], \qquad x \in \mathfrak{g}$$

(see p. 61). Therefore ad $a = 0$ if and only if $a \in \mathfrak{z}$ and hence, in view of the condition $\mathfrak{z} = 0$, if and only if $a = 0$. This means that for $\mathfrak{z} = 0$ the mapping ad is a monomorphism and hence the *Lie algebra* $\mathfrak{g}$ *is isomorphic to the linear Lie algebra* ad $\mathfrak{g}$.

To complete the proof it remains to recall (see the end of Lecture 10) that any linear Lie algebra is realizable. □

Now recall (see p. 388) that a Lie algebra $\mathfrak{h}$ is said to be an *extension* of a Lie algebra $\mathfrak{a}$ by means of a Lie algebra $\mathfrak{g}$ if $\mathfrak{a}$ is an ideal in $\mathfrak{h}$ and a Lie algebra epimorphism $\alpha\colon \mathfrak{h} \to \mathfrak{h}$ is given whose kernel is the ideal $\mathfrak{a}$. (Thus strictly speaking, not a Lie algebra $\mathfrak{h}$ but a diagram

$$0 \to \mathfrak{a} \to \mathfrak{h} \to \mathfrak{g} \to 0 \tag{1}$$

of Lie algebra homomorphisms is the extension and the diagram is *exact*, i.e. such that the kernel of each homomor-

phism in that diagram is the image of the previous homomorphism.)

Extension (1) is said to be *central* if the ideal $\mathfrak{a}$ is in the centre of $\mathfrak{h}$.

We are concerned with central extensions for which the algebra is one-dimensional and which are hence of the form

$$0 \to \mathbb{R} \to \mathfrak{h} \to \mathfrak{g} \to 0. \tag{2}$$

Such extensions are referred to as *one-dimensional.*

Proposition 1. *If the Lie algebra* $\mathfrak{g}$ *in the central one-dimensional extension* (2) *is realizable, then the Lie algebra* $\mathfrak{h}$ *is also realizable.*

The Cartan theorem is a direct consequence of this proposition. Indeed, let $\mathfrak{g}$ be a Lie algebra. Since a one-dimensional Lie algebra is realizable, it suffices to prove that $\mathfrak{g}$ is realizable if so are all Lie algebras of a smaller dimension. Since, as we have seen, a Lie algebra with $\mathfrak{z} = 0$ is realizable, it may be assumed without loss of generality that $\mathfrak{z} \neq 0$. Then for any one-dimensional subspace $\mathfrak{a}$ of the Abelian Lie algebra $\mathfrak{z}$ (which is clearly automatically an ideal of the Lie algebra $\mathfrak{g}$) the algebra $\mathfrak{g}/\mathfrak{a}$ is under the induction hypothesis realizable and hence by Proposition 1 applicable to the central extension

$$0 \to \mathfrak{a} \to \mathfrak{g} \to \mathfrak{g}/\mathfrak{a} \to 0$$

so is the Lie algebra $\mathfrak{g}$. $\square$

Thus it is only necessary to prove Proposition 1.

By analogy with the case of Lie algebras we call an *extension of a Lie group A* by means of a Lie group G an exact diagram of the form

$$1 \to A \to H \to G \to 1, \tag{3}$$

where H is a Lie group containing the group A as a closed invariant subgroup.

Extension (3) is said to be *central* if the group A is a subgroup of the centre of the group H. In this case it is convenient to call the group operation in A (not in G) an *addition* and write accordingly, instead of (3),

$$0 \to A \to H \to G \to 1.$$

As in the case of Lie algebras, we are concerned only with central extensions of the form

$$0 \to \mathbb{R} \to H \to G \to 1. \tag{4}$$

For any extension (4) the Lie algebra $\mathfrak{h} = \mathfrak{l}\,(H)$ is obviously the central one-dimensional extension (2) of the Lie algebra $\mathfrak{g} = \mathfrak{l}\,(G)$. We say that extension (2) is *realized* by extension (4).

Proposition 2. *The central extension* (2) *is realizable if so is the Lie algebra* $\mathfrak{g}$.

It is clear that Proposition 1 is a direct consequence of Proposition 2. It is only necessary therefore to prove Proposition 2.

Let G be a Lie group. *A two-dimensional cocycle* of G over $\mathbb{R}$ is a smooth function

$$f\colon\ G \times G \to \mathbb{R} \tag{5}$$

such that

$$f\,(x,\ e) = 0,\ f\,(e,\ x) = 0\ (e \text{ is the identity of } G)$$

and

$$f\,(y,\ z) - f\,(xy,\ z) + f\,(x,\ yz) - f\,(x,\ y) = 0$$

for any elements x, y, $z \in G$.

Having cocycle (5) we define on the manifold $H = \mathbb{R} \times G$ the operation of multiplication by the formula

$$(a,\ x)\,(b,\ y) = (a + b + f\,(x,\ y),\ xy),\ a,\ b \in \mathbb{R},\qquad x,\ y \in G.$$

A check shows that under this operation the manifold H is a Lie group (with identity $(0,\ e)$ and inverse element $(a,\ x)^{-1} = (-a - f\,(x,\ x^{-1}),\ x^{-1}))$. All elements of the form $(a,\ e)$ constitute a subgroup A which is isomorphic to the group $\mathbb{R}$ and is in the centre of the group G and the mapping $(a,\ x) \mapsto x$ is an epimorphism $H \to G$ with kernel A.

Thus *every cocycle* (5) *gives some central extension of the form* (4).

Remark 1. It can be shown that any central extension of the form (4) (considered up to an isomorphism identical on A and inducing an identity automorphism of G) can be

obtained in this way, two cocycles defining isomorphic extensions if and only if they are cohomologous in a natural way. We shall not need all this, however.

Remark 2. In a similar way one can describe arbitrary extensions (3) (even non-central in general). We shall not need this generalization either.

Using an exponential mapping $\exp\colon \mathfrak{g} \to G$ we call lift cocycle (5) to the Lie algebra $\mathfrak{g}$ of G, i.e. construct by the formula

$$\mathring{f}(X, Y) = f(\exp X, \exp Y), \qquad X, Y \in \mathfrak{g}$$

a smooth function

$$\mathring{f}\colon \mathfrak{g} \times \mathfrak{g} \to \mathbb{R}.$$

For this function we have

$$\mathring{f}(X, 0) = 0, \quad \mathring{f}(0, Y) = 0$$

from which it follows that

$$\text{(6)} \qquad \mathring{f}(X, Y) = c(X, Y) + \ldots$$

where c is some bilinear functional and the dots denote degrees $\geqslant 3$ in X and Y.

In addition,

$$\mathring{f}(Y, Z) - \mathring{f}(\circ(X, Y), Z) + \mathring{f}(X, \circ(Y, Z)$$
$$- \mathring{f}(X, Y) = 0$$

for any elements $X, Y, Z \in \mathfrak{g}$ from which it follows immediately that

$$c([X, Y], Z) = c(X [Y, Z]).$$

Now a calculation shows that the *functional* $u\colon \mathfrak{g} \otimes \mathfrak{g} \to \mathbb{R}$ *defined by the formula*

$$u(X, Y) = c(X, Y) - c(Y, X), \qquad X, Y \in \mathfrak{g}$$

satisfies the relation

$$u([X, Y], Z) + u([Y, Z], X) + u([Z, X], Y) = 0,$$

i.e. is a two-dimensional cocycle of $\mathfrak{g}$ over the $\mathfrak{g}$-module $\mathbb{R}$ (in the sense of Lecture 19, see the formula for δu with $m = 2$ on p. 384). We shall write $u = \mathfrak{l}(f)$.

If

$$0 \to \mathbb{R} \to H \to G \to 1 \tag{7}$$

is an extension corresponding to a cocycle f, then the elements of the Lie algebra $\mathfrak{h} = \mathfrak{l}(H)$ are naturally identified with pairs (a, X), where $a \in \mathbb{R}$ and $X \in \mathfrak{g} = \mathfrak{l}(G)$, with

$$\exp(a, X) = (a, \exp X).$$

In particular we see that the one-parameter subgroup $t \mapsto \beta_{(a,X)}(t)$ of H corresponding to an element (a, X) of $\mathfrak{h}$ is given by the formula

$$\beta_{(a,X)}(t) = (ta, \beta_X(t)),$$

where $\beta_X\colon t \mapsto \exp tX$ is a one-parameter subgroup of G corresponding to the element $X \in \mathfrak{g}$.

Therefore

$$\begin{aligned}\beta_{(a,X)}(t)\,\beta_{(b,Y)}(t) & \\ &= (ta + tb + \mathring{f}(tX, tY), \beta_X(t)\,\beta_Y(t)) \\ &= (t(a+b) + t^2 c(X, Y) + O(t^3), \beta_X(t)\,\beta_Y(t))\end{aligned}$$

for any elements $(a, X), (b, Y) \in \mathfrak{h}$ and hence

$$\begin{aligned}&\beta_{(a,X)}(t)\,\beta_{(b,Y)}(t)\,\beta_{(a,X)}(t)^{-1}\,\beta_{(b,Y)}(t)^{-1} \\ &\quad = (t^2 u(X, Y) + O(t^3), \beta_X(t)\,\beta_Y(t)\,\beta_X(t)^{-1}\beta_Y(t)^{-1}).\end{aligned}$$

It follows (see Proposition 1 of Lecture 4) that *multiplication in $\mathfrak{h}$ is given by the formula*

$$[(a, X), (b, Y)] = (u(X, Y), [X, Y]), \qquad (a, X), (b, Y) \in \mathfrak{h} \tag{8}$$

(so that, in particular, the product $[(a, X), (b, Y)]$ is independent of a and b).

Now recall (see Lecture 19, p. 389) that for any central extension of Lie algebras

$$0 \to \mathbb{R} \to \mathfrak{h} \to \mathfrak{g} \to 0 \tag{9}$$

the formula

$$u(X, Y) = [\beta X, \beta Y] - \beta [X, Y], \quad X, Y \in \mathfrak{g}, \tag{10}$$

where β: $\mathfrak{g} \to \mathfrak{h}$ is a fixed section of an epimorphism α: $\mathfrak{h} \to \mathfrak{g}$ defines some cocycle $u \in Z^2(\mathfrak{g}; \mathbb{R})$ (which is said to *classify* extension (9)). If the Lie algebra extension (9) corresponds to the Lie group extension (7), then β can be defined by the formula

$$\beta X = (0, X)$$

and hence cocycle (10) obviously coincides with the cocycle u in formula (8). Thus *for any cocycle f of the Lie group G the cocycle $u = \mathfrak{l}(f)$ classifies extension* (9) *corresponding to extension* (4) *constructed from the cocycle f.*

When the section β is changed the cocycle u is replaced, as we know (see p. 000), by a cohomologous cocycle. This means that if the central one-dimensional extensions

$$\begin{array}{c} 0 \to \mathbb{R} \to \mathfrak{h} \xrightarrow{\alpha} \mathfrak{g} \to 0 \\ \\ 0 \to \mathbb{R} \to \mathfrak{h}' \xrightarrow{\alpha'} \mathfrak{g} \to 0 \end{array} \tag{11}$$

with given sections β: $\mathfrak{g} \to \mathfrak{h}$ and β': $\mathfrak{g} \to \mathfrak{h}'$ are isomorphic (i.e. if there is an isomorphism $\mathfrak{h} \to \mathfrak{h}'$ identical on $\mathbb{R}$ and inducing an identity automorphism $\mathfrak{g} \to \mathfrak{g}$ then the corresponding cocycles u and u' are cohomologous. Conversely, let $u' - u = \delta v$, where v: $\mathfrak{g} \to \mathbb{R}$ is a cochain. Then the formula $\beta_1 X = \beta X - vX$, $X \in \mathfrak{g}$, defines a section β_1: $\mathfrak{g} \to \mathfrak{h}$ of an epimorphism α which is easily seen to have the property that the corresponding cocycle $u_1 \in Z^2(\mathfrak{g}; \mathbb{R})$ coincides with the cocycle u'. Therefore it may be assumed from the outset without loss of generality that $u = u'$. But in this case the linear mapping $\mathfrak{h} \to \mathfrak{h}'$ identical on $\mathbb{R}$ and sending every element of the form $\beta(x)$, $x \in \mathfrak{g}$, to an element $\beta'(x)$ (clearly, such a mapping exists, it is unique and an isomorphism of vector spaces which induces an identity automorphism $\mathfrak{g} \to \mathfrak{g}$) is easily seen to be an isomorphism of Lie algebras and hence extensions (11) are isomorphic.

Thus extensions (11) are *isomorphic if and only if cocycles u and u' that classify them are cohomologous.*

In particular it follows that *extension* (9) *of Lie algebras is realizable if*

(a) *the Lie algebra $\mathfrak{g}$ is realizable,*

(b) *there is a cocycle f on the group G with $\mathfrak{g}$, such that the cocycle u classifying extension* (9) *is cohomologous to the cocycle $\mathfrak{l}(f)$.*

Indeed the Lie algebra extension corresponding to extension (4) constructed with the aid of a cocycle f is known to be classified by the cocycle $\mathfrak{l}(f)$. It is therefore isomorphic to extension (9) with cohomologous cocycle u. Hence extension (9) is realizable. □

Since any realizable Lie algebra $\mathfrak{g}$ can be realized by a connected and simply connected Lie group, it follows from this statement that in order to prove Proposition 2 (and the Cartan theorem along with it) it suffices to prove Proposition 3 that follows:

Proposition 3. *If G is connected and simply connected, then for any two-dimensional cocycle $u \in Z^2(\mathfrak{g}; \mathbb{R})$ of $\mathfrak{g} = \mathfrak{l}(G)$ there is a two-dimensional cocycle f of G such that the cocycle $\mathfrak{l}(f)$ is cohomologous to u.*

Proof of Proposition 3. As we know (see pp. 402-403), there is a left-invariant form $\omega \in \Omega^2 H$ on a Lie group H, such that $u = \omega_e$. Since u is a cocycle, that form is closed. It is known (see Remarks 4 and 5 below) that *on every connected and simply connected Lie group G any closed form of degree $\leqslant 2$ is exact* (i.e. $H^1(G) = 0$ and $H^2(G) = 0$). As applied to ω this means that there is a linear form α on G, such that $\omega = d\alpha$. Although in general α is not left-invariant, it is easy to see that for any element $x \in G$ the form $L_x^*\alpha - \alpha$ is exact (indeed $d(L_x^*\alpha - \alpha) = L_x^* d\alpha - d\alpha = L_x^*\omega - \omega = 0$). Therefore for any element $x \in G$ on G there is a function φ_x such that $\varphi_x(e) = 0$ and

$$d\varphi_x = L_x^*\alpha - \alpha.$$

Since G is connected, for a fixed form α these conditions uniquely define the function φ_x. Since

$$L_{xy}^*\alpha - \alpha = L_y^*(L_x^*\alpha - \alpha) + (L_y^*\alpha - \alpha)$$

and $L_y^* d\varphi_x = dL_y^* \varphi_x$, it follows that for any two elements $x, y \in G$ we have

$$\varphi_{xy} = L_y^* \varphi_x + \varphi_y - \varphi_x(y),$$

i.e.

$$\varphi_{xy}(z) = \varphi_x(yz) + \varphi_y(z) - \varphi_x(y), \quad z \in G.$$

On putting now

$$f(x, y) = \varphi_x(y)$$

we get, first,

$$f(x, e) = \varphi_x(e) = 0, \quad f(e, x) = \varphi_e(x) = 0$$

(clearly, $\varphi_e = 0$) and, secondly,

$$f(y, z) - f(xy, z) + f(x, yz) - f(x, y) = 0.$$

Hence the function f: $G \times G \to \mathbb{R}$ (obviously smooth) is a two-dimensional cocycle on G.

For the proof of Proposition 3 to be complete it thus remains merely to prove that the *cocycle* $\mathfrak{l}(f)$ *is cohomologous to* u.

Recall that the *Lie derivative* of an (a, b)-tensor field T along a vector field X (on a manifold M) is an (a, b)-tensor field $\mathscr{L}T$ taking at a point $p \in M$ a value

$$(\mathscr{L}_X T)_p = \lim_{t \to 0} \frac{(\alpha_t^* T)_p - T_p}{t}, \tag{12}$$

where α_t: $\mathscr{M} \to \mathscr{M}$ is a flux on $\mathscr{M}$ (in general local) generated by the field X (i.e. a family of diffeomorphisms α_t: $\mathscr{M} \to \mathscr{M}$ such that for any point $p \in \mathscr{M}$ the tangent vector to the curve $t \to \alpha_t(p)$ at p is the vector X_p). In the case (the only one necessary), where $\mathscr{M}$ is a Lie group G and the field X is left-invariant, formula (12) becomes

$$(\mathscr{L}_X T)_p = \lim_{t \to 0} \frac{(L_{\exp tX}^* T)_p - T_p}{t}.$$

For example, if T is a function φ: $G \to \mathbb{R}$, then $\mathscr{L}_X \varphi$ is also a function and

$$(\mathscr{L}_X \varphi)(p) = \lim_{t \to 0} \frac{\varphi(\exp tX \cdot p) - \varphi(p)}{t},$$

that is

$$(13) \qquad (\mathscr{L}_X\varphi)(p) = \left.\frac{d\varphi(\exp tX\cdot p)}{dt}\right|_{t=0}$$

for any point $p \in G$. On the other hand, since the tangent vector to the curve $t \mapsto \exp tX\cdot p$ at a point p is the vector X_p, we have

$$\left.\frac{d\varphi(\exp tX\cdot p)}{dt}\right|_{t=0} = X_p\varphi,$$

and since by the definition of the differential of a function

$$X_p\varphi = d\varphi_p(X_p) = (d\varphi(X)(p),$$

we finally have

$$(14) \qquad \mathscr{L}_X\varphi = d\varphi(X).$$

For a form ω of degree $r > 0$ and a field X the form $(X_1, \ldots, X_{r-1}) \mapsto \omega(X, X_1, \ldots, X_{r-1})$ of degree $r-1$ is denoted by the symbol $X \lrcorner\, \omega$. In this notation formula (14) becomes

$$\mathscr{L}_X\varphi = X \lrcorner\, \varphi.$$

[Note that although we have proved the validity of that formula only for the left-invariant field X on the group G, it holds in fact, with the proof practically the same, for an arbitrary field X on an arbitrary smooth manifold $\mathscr{M}$.]

Formula (13) can be readily extended to differential forms of arbitrary degree. That is, it turns out (see Remark 6 below) that *for any differential form* ω *there is an identity*

$$(14) \qquad \mathscr{L}_X\omega = X \lrcorner\, d\omega + d(X \lrcorner\, \omega),$$

going over into identity (13) when $\deg \omega = 0$.

Equipped with this information we can now proceed directly to the proof that the cocycles $\mathfrak{l}(f)$ and u are cohomologous.

By definition

$$\mathring{f}(tX, sY) = \varphi_{\exp tX}(\exp sY)$$

for any $t, s \in \mathbb{R}$. So by formulas (13) and (14)

$$\left.\frac{\partial \mathring{f}(tX, sY)}{\partial s}\right|_{s=0} = (d\varphi_{\exp tX})(Y)(e),$$

i.e.

$$\left.\frac{\partial \overset{\circ}{f}(tX, sY)}{\partial s}\right|_{s=0} = (L^*_{\exp tX}\alpha - \alpha)(Y)(e)$$

and hence

$$\left.\frac{\partial^2 \overset{\bullet}{f}(tX, sY)}{\partial t\, \partial s}\right|_{\substack{t=0\\ s=0}} = (\mathcal{L}_X\alpha)(Y)(e)$$

$$= (X \lrcorner\, d\alpha + d(X \lrcorner\, \alpha))(Y)(e)$$

$$= d\alpha(X, Y)(e) + d(\alpha(X))(Y)(e).$$

By construction, $d\alpha = \omega$ and $\omega_e = u$. Therefore

$$d\alpha(X, Y)(e) = (d\alpha)_e(X_e, Y_e) = u(X, Y)$$

(in the last transformation we have identified X_e with X and Y_e with Y). Since

$$d(\alpha(X))(Y) = Y\alpha(X),$$

this proves that

$$\left.\frac{\partial \overset{\circ}{f}(tX, sY)}{\partial s\, \partial t}\right|_{\substack{t=0\\ s=0}} = u(X, Y) + Y\alpha(X)(e)$$

for any left-invariant fields $X, Y \in \mathfrak{g}$.

On the other hand, if

$$\overset{\circ}{f}(X, Y) = c(X, Y) + \ldots,$$

where the dots denote terms of degree $\geqslant 3$ in X and Y, then

$$\left.\frac{\partial \overset{\circ}{f}(tX, sY)}{\partial t\, \partial s}\right|_{\substack{t=0\\ s=0}} = c(X, Y).$$

Hence

$$c(X, Y) = u(X, Y) + Y\alpha(X)(e),$$

from which it follows (since $u(Y, X) = -u(X, Y)$) that

$$\mathfrak{l}(f)(X, Y) = 2u(X, Y) + (Y\alpha(X) - X\alpha(Y))(e).$$

Since by formula (3) of Lecture 20

$$\omega(X, Y) = d\alpha(X, Y) = X\alpha(Y) - Y\alpha(X) - \alpha[X, Y]$$

and $\omega(X, Y)(e) = u(X, Y)$, this proves that

$$\mathfrak{l}(f)(X, Y) = u(X, Y) + \alpha[X, Y](e),$$

i.e. that

$$\mathfrak{l}(f) = u - \delta v,$$

where v is a cochain $\mathfrak{g} \to \mathbb{R}$ defined by the formula

$$vX = \alpha(X)(e)$$

for any element $X \in \mathfrak{g}$.

Thus the cocycles $\mathfrak{l}(f)$ and u are in fact cohomologous. □

Remark 3. All the steps in the reduction of the Cartan theorem to Proposition 3 have been known for over thirty years now. Proposition 3 was first proved by Pinchon and Simon in 1975 using a general theory. We owe to Gorbatsevich not only the idea of applying Proposition 3 to the proof of the Cartan theorem but also the above elementary proof of the proposition.

Remark 4. The equation $H^1(\mathcal{M}) = 0$ holds for an arbitrarily connected and simply connected manifold $\mathcal{M}$. Indeed, it follows from the simple connectedness of $\mathcal{M}$, by the Stokes formula, that for any closed linear differential form α and any closed path $\gamma: [0, 1] \to \mathcal{M}$ on $\mathcal{M}$ the integral $\oint_\gamma \alpha$ is zero. Therefore by choosing a point $p_0 \in \mathcal{M}$ and putting for every point $p \in \mathcal{M}$

$$f(p) = \oint_\gamma \alpha,$$

where γ is a path joining points p_0 and p, we correctly define on $\mathcal{M}$ a function f with the property that $df = \alpha$.

Remark 5. For a manifold $\mathcal{M}$ the direct sum

$$H^*(\mathcal{M}) = \bigoplus_{m=0}^{\dim M} H^m(\mathcal{M})$$

of cohomology groups is an associative and anticommutative graded algebra with respect to a multiplication defined (as one can easily see, correctly) by the formula

$$[\omega_1] \wedge [\omega_2] = [\omega_1 \wedge \omega_2],$$

where $[\omega]$ denotes a class of cohomologies of the closed form ω. Since $H^m(M) = 0$ for $m > \dim M$, *homogeneous elements of the algebra* $H^*(\mathcal{M})$ *of positive degree are all nilpotent.* If $\mathcal{M}$ is a Lie group G, then the multiplication $G \times G \to G$ induces a mapping

$$\delta\colon H^*(G) \to H^*(G \times G) \approx H^*(G) \times H^*(G)$$

with respect to which the algebra $H^*(G)$ is a Hopf algebra. If $H^1(G) = 0$, then any element of the group $H^2(G)$ is primitive in an obvious way. For a connected and simply connected Lie group G therefore the equation $H^2(G) = 0$ follows from this general-algebraic lemma:

Lemma. *In an associative and anticommutative Hopf algebra* $\mathcal{A}$ *every nilpotent primitive element* a *of even degree is zero.*

Proof. Since $\delta a = 1 \oplus a + a \oplus 1$, we have

$$\delta a^n = \sum_{m=0}^{n} \binom{n}{m} a^m \oplus a^{n-m}.$$

Since bidegrees of all elements $a^m \oplus a^{n-m}$ are distinct, it follows that the equation $a^n = 0$ is possible only when for any $m = 0, \ldots, n$ we have $a^m \oplus a^{n-m} = 0$ and hence (for $x \oplus y = 0$ is possible in $\mathcal{A} \otimes \mathcal{A}$ only when either $x = 0$ or $y = 0$) for $m > 0$ we also have $a^m = 0$. At $m = 1$ we thus get $a = 0$. $\square$

Remark 6. The operation $\mathcal{L}_X$ on forms is obviously commutative with the operation of external differentiation d, i.e.

$$d\mathcal{L}_X\omega = \mathcal{L}_X d\omega$$

for any form ω and is a differentiation with respect to the external multiplication of forms, i.e.

$$\mathcal{L}_X(\omega_1 \wedge \omega_2) = \mathcal{L}_X\omega_1 \wedge \omega_2 + \omega_1 \wedge \mathcal{L}_X\omega_2$$

for any forms ω_1 and ω_2.

On the other hand, a calculation, which uses the fact that the operators d and $X \lrcorner$ are both *antidifferentiations*, shows that the operator

$$\omega \mapsto X \lrcorner\, d\omega + d(X \lrcorner\, \omega)$$

is also a differentiation. Since two differentiations coincide if they coincide on the generators, it follows that it suffices to prove formula (14) for forms ω which are functions and for forms of the type dx^i, where $x^1, \ldots, x^n$ are local coordinates.

For the functions formula (14) reduces to the already known formula (13) and for the forms of the type dx^i it is as follows

$$\mathcal{L}_X \, dx^i = d\,(X \lrcorner \, dx^i) = dX^i,$$

where X^i is a component of the vector field X in a chart with local coordinates $x^1, \ldots, x^n$.

If $\alpha_t^i(X)$ are the coordinates of a point $\alpha_t(p)$, where $\{\alpha_t\}$ is a flux generated by the field X (i.e. the coordinates of the point $\exp tX \cdot p$, in the case of Lie groups of interest here), then by definition

$$\begin{aligned}
\mathcal{L}_X \, dx^i &= \lim_{t\to 0} \frac{\dfrac{\partial \alpha_t^i(X)}{\partial x^j}\, dx^j - dx^i}{t} \\
&= \lim_{t\to 0} \frac{1}{t}\left(\frac{\partial \alpha_t^i(X)}{\partial x^j} - \delta_j^i\right) dx^j \\
&= \frac{\partial}{\partial t}\left(\frac{\partial \alpha_t^i(X)}{\partial x^j}\right)\Bigg|_{t=0} dx^j \\
&= \frac{\partial}{\partial x^j}\left(\frac{\partial \alpha_t^i(X)}{\partial t}\Bigg|_{t=0}\right) dx^j \\
&= \frac{\partial X^i}{\partial x^j}\, dx^j = dX^j,
\end{aligned}$$

since $\dfrac{\partial \alpha_t^i(X)}{\partial t}\Bigg|_{t=0} = X^i$.

This completes the proof of formula (14) (on any chart and hence everywhere). □

BIBLIOGRAPHY

1. N. Bourbaki, *Eléments de Mathématique, Groupes et algèbres de Lie*, Chapitre 1: Algèbres de Lie, Hermann, Paris, 1960; Chapitre 2: Algèbres de Lie libres. Chapitre 3: Groupes de Lie, Hermann, Paris, 1972.
   A modern detailed exposition, very difficult to read.
2. N.G. Chebotaryov, *The Theory of Lie Groups*, Gostekhizdat, Moscow and Leningrad, 1940 (In Russian).
   The earliest Russian monograph on Lie group theory. A classical exposition in the spirit of Lie himself and Cartan. It is quite obsolete now, but some chapters may be of interest even today.
3. Cl. Chevalley, *Theory of Lie Groups.*, I, Princeton University Press, Princeton, 1946.
   An early and very successful attempt at a modern exposition of the theory. In particular it contains the earliest accurate theory of integrable subfiberings (see Lectures 7 and 11) and covering space theory using no paths (Lecture 8).
4. J. Dixmier, *Algèbres enveloppantes*, Paris, Bruxsseles, Montréal, 1974.
   The first chapter of this book is a well thought-out, although brief, account of a number of questions of Lie algebra theory. Lecture 17 of our course uses the proof of Cartan's criterion for solvability given in this book.
5. E.B. Dynkin, Normed Lie algebras and analytic groups, *Amer. Math. Soc. Transl.* (1) 9, 470-534.
   A detailed exposition of the author's results on the explicit calculation of the Campbell-Hausdorff series (Lecture 5). Also presented is the application of these calculations to the construction of a local Lie group from a Lie algebra (Lecture 6).
6. V.M. Glushkov, The structure of locally bicompact groups and Hilbert's fifth problem, *Uspekhi Mat. Nauk*, 12, No. 2 (74), 3-41 (1957).
   A detailed exposition of Hilbert's fifth problem.
7. N. Jacobson, *Lie Algebras*, Interscience Publishers, New York and London, 1962.
   A detailed monograph, rather difficult to read. The scheme of the proof of the Ado theorem in Lecture 19 is taken from this book.
8. I. Kaplansky, *Lie Algebras and Locally Compact Groups*, The University of Chicago Press, Chicago and London, 1971.
   This book has two practically independent parts. The first is a general algebra theory-oriented exposition of the elements of Lie algebra theory. We use this exposition in Lecture 16. The second part is devoted to the solution of Hilbert's fifth problem.
9. L.S. Pontryagin, *Topological Groups*, 2nd ed., Gordon and Breach, New York, 1966.
   A classical monograph on the theory of topological and smooth groups. As regards Lie groups it contains essentially all the material of the present lectures; but Lie's third theorem (the equivalence of GR-LOC and ALC_{f}-LIE) is proved in this book by an entirely different method (close to that of Lie himself),

and the Cartan theorem (the equivalence of GR_{00}-DIFF and ALG_f-LIE) is proved only modulo the Levi theorem which is taken for granted. It should be kept in mind that the 1938 GONTI and 1954 Gostekhizdat editions of this book contain an uncertainty in the proof of Lie's third theorem.

10. J.-P. Serre, *Lie Algebras and Lie Groups*, New York and Amsterdam, 1965; *Algèbres de Lie. Semi-simples complexes*, New York and Amsterdam, 1966.
A rather complete and detailed exposition intended for the prepared reader.

Secondary

11. H. Freudenthal, *Oktaven, Ausnahmgruppen und Oktavengeometrie*, Mathematisch Instituut der Rigksuniversiteit te Utrecht, 1951.
Presentation of the author's studies of the groups G_2, F_4 and E_6 and related questions. It is intended for specialists. It is very difficult to read because of the obsolete terminology and some peculiarities of the author's style.
12. I.L. Kantor, A.S. Solodovnikov, *Hypercomplex numbers*. Nauka, Moscow, 1973.
A popular introduction to the theory of quaternions and octaves, contains a proof of the Hurwitz and the Frobenius theorem.
13. W.S. Massey, J. Stollings, *Algberaic Topology: An Introduction*, New York, Chicago, San Francisco, Atlanta, 1967.
A detailed exposition for beginners of the theory of covering spaces and fundamental groups in the "classical spirit", i.e. using the concept of a homotopy of continuous paths.

SUBJECT INDEX

Ado theorem, 207
Algebra, alternative, 293
  associative, algebraic element of, 408
  free, 98
  invertible element of, 44
  Jordan, 323
  normed, 288
  of double numbers, 256
  of dual numbers, 256
  of octaves (of Cayley numbers), 293
  of polynomials, 98
  in noncommuting unknowns, 98
  over a field, 43
  associative, 44
  universal enveloping, 104
  Z_2-graded, 251
Antiautomorphism of an algebra, involutory, 258
Associator, 307

Cain group, 393
Campbell-Hausdorff series, 76
  in the Dynkin form, 124
Cartan's criterion, for semisimplicity, 374
  for solvability, 365, 368
Cartan theorem, 136, 202, 231
Casimir operator, 375
Categories, of coverings, 181
  equivalent, 131
Category, of coverings, 170
  of pointed coverings, 171
Cayley algebra, 293
Cayley construction, 22
Cayley image, of a group, 22
  of a matrix, 20
Cayley number, 293
Centre, of a Lie algebra, 349
  of an associative algebra, 258
Chart, canonical, 93
Clifford algebra, 249
  element of, even, 251
  odd, 251
Clifford group of degree n and index ε, 259
Coalgebra, 114
Coamalgam, 165, 173, 176
Coboundary, 379
Cochain, 377
Cocycle, 379
Coidentity, 114
Commutator Lie algebra, 60
Commutator of two elements of an associative algebra, 60
Component of arcwise connectedness, 27
Comultiplication, 114
Configuration, F_4, 343
  G_2, 301
Conjugation, of a Clifford algebra, 258
  of a finite-dimensional algebra over $\mathbb{R}$, 286
Constants, structural, 298
Coordinates
  canonical 93

Coordinates
of the first kind 94
of the second kind 94
normal 83
Covering, 159
pointed, 165
maximal, 172
simply connected, 172
universal, 172
smooth, 183
trivial, 168
weak, 160
Coverings, pointed equivalent, 172
Curve of a vector field
integral, 36
maximal, 36

Decomposition of a representation into a direct sum, 383
Degree, of a monomial, 99
of a linear operator, external pth, 283
Diagonal mapping, 114
Differentiation of an algebra, 61
interior 61
Differentiations, adjoint, 333
Doubling of an algebra, 286
Dynkin polynomial, 78
Dynkin's theorem, 123

Element, primitive, 114
special, 108
Engel theorem, 354
Extension of Lie algebras, 388
central, 419
trivial, 388

Factor group, local, 140
Fibering, induced, 144
Fitting decomposition of a linear operator, 383
Freudenthal theorem, 333
Friedrichs' theorem, 118
Frobenius theorem, 148
generalized, 295
Function in an algebra, derived, 47
exponential, 47
Functional, bilinear invariant, 360
Killing's, 361
Functor, completely univalent, 142
Functors, quasi-inverse, 131

Germ, of local Lie groups, 68
of homomorphisms, 69
Graph of the Pfaffian system, 145
Group, admitting the Cayley construction, 22
algebraic, 232
fundamental, 192
local, embeddable, 204
globalizable, 204
Group (Cont.)
locally flat, 97
of unimodular unitary matrices, 32
orthogonal symplectic, 24
real linear symplectic, 23
simply-connected covering, 196
smooth, 15
symplectic, 26
topological, 16
without small subgroups, 96
unitary, 25
symplectic, 26
Group covering, 189

Hausdorff (separable) topological space, 16

Homomorphism, continuous, 16
local, 160
Homomorphism, of algebras, 43
of Lie groups, smooth, 15
of local Lie groups, 69
Hopf algebra, 114

Ideal of a Lie algebra, 138
characteristic, 406
Idempotent, 324
primitive, 324
Integral of a Pfaffian system, 144
Identity, 67
of elasticity, 307
Identity element, 67
Immersion, 228
Isomorphism of topological groups, local, 194

Jacobi identity, 60
Jacobson theorem, 352
Jordan decomposition of a linear operator, 366

Killing's functional, 361
Kronecker product of matrices, 276

Lagrange theorem, 254
Leibnitz formula, 233
Levi theorem, 391
Lie algebra, 60
Abelian, 349
f_4, 330
free, 98
g_2, 296
linear, 351
irreducible, 356
nilpotent, 349
of a Lie group, 63
of a local group, 69
of vector fields on a manifold, 62
realizable, 418
reductive, 357
semisimple, 348
simple, 392
solvable, 347
Lie bracket, 60
of vector fields, 62
Lie correspondence, 136, 209
Lie functor, 41, 66, 70, 130
Lie group, 15
local, 67
analytic, 142
smooth, 142
Lie group algebra, 129
Lie group F_2, 330
Lie group G_2, 296
Lie groups, equivalent local, 68
locally isomorphic, 66
Lie monomial, 120
Lie nilsubalgebra, 351
Lie polynomial, 76, 100
Lie subgroup, 209
Lie's third theorem, 133
Linearization, 306
Local factor group, 140
Local group, embeddable, 204
globalizable, 204
Local Lie group, 67
analytic, 142
smooth, 142
Local Lie groups, equivalent, 68
Local subgroups, 134
invariant, 138
locally flat, 135
Localization functor, 69

Manifold, integral, 210
maximal, 212
parallelizable, 35

Mapping, smooth, 17
Matrix, complex orthogonal, 25
complex symplectic, 25
J-orthogonal, 23
J-skew-symmetric, 23
J-unitary, 25
monomial, 276
nonexceptional, 20
octave, skew-Hermitian, 331
Hermitian, 322
symplectic, 22
unitary, 25
Matrix algebra, 44
Matrix function, exponential, 47
Matrix Lie group, 51
Matrix representations, equivalent, 275
Metric algebra, 288
Module over a Lie algebra, 103
Monomial, 99
empty, 99
Morphism, of Lie groups, 15
of coverings, 170
Moufang identity, central, 314
right, 315

Neighbourhood, canonical, 93
normal, 74
Nilrepresentation of a Lie algebra, 412
Nilradical of a Lie algebra, 351
Norm in an algebra, multiplicative, 45

Object of a category, initial, 248
Octave, 293
One-parameter subgroup, 38

Part, of a local group, 68
of a linear operator, diagonalizable, 366
nilpotent, 366
Path, 27
Plane, projective octave, 326
Poincaré group, 192
Poinaré-Birkhoff theorem, 111
Polarization, 306
Polynomial, noncommutative, 76
Problem, Hilbert's fifth, 97
Product, left internal, 282
of ideals, 403
right internal, 283
Property, of naturalness, 73
of being universal, 104

Quotient algebra of a Lie algebra mod an ideal, 140
Quotient manifold, 239

Radical of a Lie algebra, 348
nilpotent, 359
Rank of a smooth mapping, 214
Representation, of a Lie algebra, 364
adjoint, 364
of a Lie group, adjoint, 86
semispinor, 280
Restriction, 145

Shift, left, 19
right, 19
Shifts by an element a, 19
Solenoid (group), irrational, 208
Space, arcwise connected topological, 27
connected topological, 27
homogeneous, 239
locally (arcwise) connected topological, 27
locally simply connected topological, 185
of a representation of a Lie algebra, 364
pointed topological, 165

Space
semilocally simply connected topological, 173
simply connected topological, 169
Spinor group of degree n and index ε, 259
Spinor representation, 280
Square, dissected, 218
universal, 165
Subalgebras of an algebra, 44
Subcategory, complete, 44
Subfibering, completely integrable, 151
involutory, 151
of a tangent fibering (or bundle), 145
Subgroup, discrete, 194
of a Lie group, 209
invariant, 209
possessing an ln-image, 58
Subgroups, invariant local, 138
locally flat local, 135
Submanifold, 208
Subset, evenly covered by a mapping, 159
locally closed, 230
of a group, small, 198
of the product of two groups, distinguished, 198
Subspace (subalgebra), associatively nilpotent, 351
System, Pfaffian, 143
integrable, 144

Tensor product, of algebras, 113
of vector spaces, 112
of Z_2-graded algebras, skew, 253
Trace functional, of a Lie algebra, 360
of a representation of a Lie algebra, 364
Triplicity principle, for group Spin (8), 316
infinitesimal 316
Triproduct, scalar, 329

Unit sphere, 20

Variety, algebraic, 232
Vector field, complete, 37
on a group, left invariant, 34
on a manifold, 33
Vector fields, Φ-connected, 41

Waring formulas, 355
Weyl theorem, 386
Whitehead's theorem, 380
Whitehead's lemma, first, 385
second, 386

TO THE READER

Mir Publishers would be grateful for your comments on the content, translation and design of this book.

We would also be pleased to receive any other suggestions you may wish to make.

Our address is:
Mir Publishers
2 Pervy Rizhsky Pereulok
I-110, GSP, Moscow, 129820
USSR

Printed in the Union of Soviet Socialist Republics

A Problem-Book in Differential Geometry and Topology

A. MISHCHENKO, D.Sc. (Phys.-Math.),
Yu. SOLOVYEV, Cand. Sc. (Phys.-Math.),
and A. FOMENKO, D.Sc. (Phys.-Math.)

This problem book was compiled by three eminent Moscow University teachers. Based on many years of experience at the mechanics-and-mathematics department, it contains problems for practically all the sections of the differential geometry and topology course delivered to students at the University. Besides the classic branches of the theory of curves and surfaces, the reader will be offered problems in smooth manifold theory, Riemann geometry, vector fields and differential forms, general and homotopical topology, and in the elements of variational calculus. The structure of the problem book corresponds to 'A Course of Differential Geometry and Topology' (Moscow University Press, 1980) by Prof. A. S. Mishchenko and Prof. A. T. Fomenko. Some problems, however, touch upon topics outside the course of lectures. These sections are provided then with all the necessary theoretical foundations, hints and answers.

УДК 513(075.8)=20

Учебное пособие

Михаил Михайлович Постников

ЛЕКЦИИ ПО ГЕОМЕТРИИ

СЕМЕСТР V

ГРУППЫ И АЛГЕБРЫ ЛИ

Научный редактор Г. Б. Рыбчинская
Контрольный редактро Г. Г. Анохина
Редакторы Р. И. Алавина, Н. Ф. Шлифер
Художник Н. В. Зотова
Технический редактор В. П. Сизова
Корректоры Н. Ф. Шлифер, М. Э. Александрова

ИБ № 5664

Сдано в набор 02.12.85. Подписано к печати 22.05.86.
Формат $84 \times 108^{1}/_{32}$. Бумага типографская № 1.
Печать высокая. Гарнитура обыкновенная. Объем 6,88 бум. л.
Усл. печ. л. 23,10. Усл. кр.-отт. 23,47. Уч.-изд. л. 22,68.
Изд. № 10/3948. Тираж 7470 экз. Зак. 0450. Цена 2 р. 16 к.

ИЗДАТЕЛЬСТВО «МИР»
129820, ГСП, Москва, И-110, 1-й Рижский пер., 2.

Ордена Трудового Красного Знамени
Московская типография № 7 «Искра революции»
Союзполиграфпрома Государственного комитета СССР
по делам издательств, полиграфии и книжной торговли.
103001, Москва, Трехпрудный пер., 9.

$\text{П}\,\dfrac{056(01)-86}{1702040000-311}\,6\text{—}86$, ч. 2

M. Postnikov received his doctor's degree (Phys.-Math.) in 1954, from 1955 to 1960 was Professor of the Higher Algebra Department, and since 1965 he has been Professor of the Higher Geometry and Topology Department (Moscow State University).

He is a senior research worker at the Steklov Institute of Mathematics. In 1961, Prof. Postnikov was awarded Lenin Prize for a series of works on the homotopy theory of continuous maps. He is the author of several monographs and textbooks some of which have been translated into foreign languages.

LECTURES IN GEOMETRY

Semester 1

ANALYTIC GEOMETRY

M. Postnikov

This textbook comprises lectures read by the author to the first-year students of mathematics at Moscow State University. The book is divided into two parts containing the texts of lectures read in the first and second semesters, respectively.

Part One contains 29 lectures, and is read in the first semester.

The subject matter is presented on the basis of vector axiomatics of geometry with special emphasis on logical sequence in the introduction of the basic geometrical concepts.

Systematic exposition and application of bivectors and trivectors enables the author to successfully combine the above course of lectures with those of the following semesters.

The book is intended for university undergraduates majoring in mathematics.

$$\begin{tikzcd} \widetilde{H} \arrow[r, dash] \arrow[d, "\pi_H"'] & {} \\ H \arrow[r, dash] & {} \end{tikzcd}$$